MARCO ESTRATÉGICO DE GESTIÓN PARA LA CONTINUIDAD DE LOS SERVICIOS DE TI EN INSTITUCIONES UNIVERSITARIAS PRIVADAS COLOMBIANAS.

CASO DE ESTUDIO: UNIVERSIDAD DEL NORTE

CARLOS ANDRÉS CARO PÉREZ

MILAGRO ISABEL SANJUÁN CAMACHO

FUNDACIÓN UNIVERSIDAD DEL NORTE

DIVISIÓN DE INGENIERÍAS

MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA

BARRANQUILLA

2018

MARCO ESTRATÉGICO DE GESTIÓN PARA LA CONTINUIDAD DE LOS SERVICIOS DE TI EN INSTITUCIONES UNIVERSITARIAS PRIVADAS COLOMBIANAS.

CASO DE ESTUDIO: UNIVERSIDAD DEL NORTE

CARLOS ANDRÉS CARO PÉREZ

MILAGRO ISABEL SANJUÁN CAMACHO

Proyecto presentado como requisito para optar el título de Magíster en Gobierno de Tecnología Informática.

Tutor:

Ing. WILSON NIETO BERNAL

Doctor en Ciencias de la computación

ULPCG España

FUNDACIÓN UNIVERSIDAD DEL NORTE

DIVISIÓN DE INGENIERÍAS

MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA

BARRANQUILLA

2018

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma presidente del Jurado

_____

Firma Jurado 1

_____

Firma Jurado 2

TABLA DE CONTENIDO

1. INTRODUCCIÓN 8
2. DESCRIPCIÓN DEL PROBLEMA 10
3. JUSTIFICACIÓN 12
4. OBJETIVOS 13
4.1 OBJETIVO GENERAL 13
4.2 OBJETIVO ESPECÍFICOS 13
5. METODOLOGÍA 14
5.1 TIPO DE INVESTIGACIÓN 14
5.2 PERIODO Y LUGAR 14
5.3 MÉTODO 14
5.4 ACTIVIDADES 15
6. ALCANCE 16
7. MARCO CONCEPTUAL 17
7.1 RESILIENCIA 17
7.1.1 Resiliencia operativa y continuidad de servicios de TI 17
7.2 GOBIERNO CORPORATIVO 17
7.3 GOBIERNO DE TI 19
7.3.1 Propósito del gobierno de TI - Gad j Selig (2008) 20
7.3.2 Alcance del gobierno de TI - Gad j Selig (2008) 20
7.4 FRAMEWORK INTEGRADO DE TI 23
7.5 ESTRATEGIA DE TI 26
7.6 SISTEMA DE GESTIÓN 26
7.6.1 Círculo de Deming: 26
8. MARCO REFERENCIAL 29
8.1 COBIT 29
8.1.1 Introducción marco de Cobit 29
8.1.2 Cobit 5 30
8.1.3 Principios de Cobit 5 30
8.1.4 Procesos de gobierno y gestión 31
8.2 ITIL 35

8.2.1 Estrategia del servicio 36
8.2.2 Diseño del servicio 37
8.2.3 Transición del servicio 38
8.2.4 Operación del servicio 38
8.2.5 Mejora continua del servicio 39
9. MODELO PROPUESTO 41
9.1 DESCRIPCIÓN DEL MODELO 41
9.1.1 Planeación 42
9.1.1.1 Gestionar el Marco de Gestión de TI 42
9.1.1.2 Gestionar la Estrategia 43
9.1.1.3 Gestionar los Acuerdos de Servicio 44
9.1.1.4 Gestionar el Riesgo 45
9.1.1.5 Gestionar la Seguridad 45
9.1.2 Construir, Adquirir y Diseñar 46
9.1.2.1 Gestionar la Definición de Requisitos 46
9.1.2.2 Gestionar la Identificación y la Construcción de Soluciones 47
9.1.2.3 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos 48
9.1.3 Implementar 49
9.1.3.1 Gestionar los Programas y Proyectos 49
9.1.3.2 Gestionar los Cambios 50
9.1.3.3 Gestionar la Configuración 51
9.1.4 Operar 52
9.1.4.1 Gestionar las Operaciones 52
9.1.4.2 Gestionar las Peticiones y los Incidentes del Servicio 53
9.1.4.3 Gestionar la Continuidad 54
9.1.4.4 Gestionar la Disponibilidad y la Capacidad 56
9.2 MÉTRICAS 56
9.3 ROLES 59
9.4 MEDICIÓN DE NIVEL DE MADUREZ 60
10. CASO DE ESTUDIO 63
10.1 UNIVERSIDAD DEL NORTE 63
10.1.1 Caracterización Organización 63
10.1.1.1 Misión 63

10.1.1.2 Visión 65
10.1.1.3 Gobierno Corporativo 66
10.1.1.4 Estado Actual de GyG-TI 67
10.2 MEDICIÓN DE MADUREZ DE LA ORGANIZACIÓN DEL MODELO PROPUESTO 70
10.2.1 Medición de la madurez inicial 70
10.2.2 Análisis de brechas evaluación inicial 72
10.2.3 Medición de la madurez después de la aplicación del plan de trabajo inicial 72
1. CONCLUSIONES 75
BIBLIOGRAFÍA 76
ANEXO 1. FORMULARIO EVALUACIÓN INICIAL UNINORTE 78
ANEXO 2. FORMULARIO EVALUACIÓN POSTERIOR AL PLAN DE TRABAJO UNINORTE 80

LISTA DE TABLAS

Tabla 1. Diferencias entre los gobiernos corporativo, empresarial y de TI en el contexto de la Universidades privadas. 18
Tabla 2. Marco de Gobierno de TI integrado 25
Tabla 3. Procesos de Gobierno 32
Tabla 4. Proceso de Gestión - APO 32
Tabla 5. Proceso de gestión - BAI 33
Tabla 6. Proceso de gestión - DSS 33
Tabla 7. Proceso de gestión - MEA 34
Tabla 8. MEGCS 42
Tabla 9.Métricas 57
Tabla 10.Criterios de evaluación nivel de madurez 60
Tabla 11.Criterios de evaluación nivel de madurez 62
Tabla 12.Evaluación inicial Uninorte 71
Tabla 13. Evaluación posterior Uninorte 73

LISTA DE FIGURAS

Figura 1. Ciclo de mejora continúa 25
Figura 2. Principios de Cobit 5..... 32
Figura 3. Procesos de Gobierno y Gestión de TI de Cobit 5..... 32
Figura 4. Ciclo de vida del servicio..... 33
Figura 5. Marco estratégico de gestión para la continuidad de los servicios de TI en instituciones universitarias privadas en Colombia 33
Figura 6. Organigrama de la Universidad del Norte 34
Figura 7. Organigrama de la Dirección de TI de la Universidad del Norte 34
Figura 8. Medición de madurez inicial..... 71
Figura 9. Medición de madurez después del plan de trabajo inicial 34

1. INTRODUCCIÓN

Una institución universitaria privada en Colombia tiene la necesidad de garantizar la pronta recuperación de sus actividades de negocio, es decir, garantizar la continuidad del entorno de aprendizaje ante la amenaza u ocurrencia de cualquier tipo de evento adverso o negativo que afecte su normal funcionamiento. Cuando hablamos de eventos adversos o negativos que pueden llegar a tener un impacto en la continuidad de los servicios de la institución, se hace referencia a desastres naturales, actos de terrorismo, ciberataques, interrupciones no planificadas en TI y telecomunicaciones, caídas de los sistemas eléctricos, entre otros.

Para lograr asegurar la continuidad de la operación de una empresa o de una institución universitaria, existen diferentes normas internacionales como BSI 25999 y la ISO 22301. La norma BSI 25999 tiene como objeto la gestión del plan de continuidad del negocio y la norma ISO 22301 se encarga de establecer requisitos que permitan minimizar el impacto de aquellos incidentes que generen una interrupción en las actividades. Sin embargo, una empresa o institución universitaria no solo asegura la continuidad de las operaciones del negocio teniendo un SGCN, ya que el uso de la tecnología de información para soportar sus servicios críticos se ha vuelto vital en los últimos años. Por lo cual, existen estándares y normas internacionales que ayudan a la gestión de la continuidad de los servicios de TI, como el publicado en el 2008 por la British Standards Institution (BSI) BS 25777:2008, Gestión de la Continuidad de las TIC, un estándar que alineado con el BS 25999 define un conjunto de mejores prácticas sobre la continuidad, centrado en la infraestructura TIC de la organización. Cobit 5 como marco efectivo de Gobierno y Administración de las TI en la organización, que a través de su proceso DSS04 Gestionar la continuidad del servicio, brinda los lineamientos

para entregar, servir y dar soporte de manera continua; ITIL V3 como marco de mejores prácticas para la gestión del ciclo de vida del servicio contempla en su estrategia de diseño del servicio la Gestión de continuidad de servicios de TI (ITSCM) que su principal objetivo es minimizar el impacto ante una imprevista interrupción de los servicios a causa de desastres naturales.

De lo anterior, se evidencia que la continuidad de los servicios TIC cobran gran relevancia para el negocio. Entonces, las instituciones universitarias privadas en Colombia deben definir también estrategias que le permitan gestionarla. Estas estrategias deben ir apalancadas con la implementación de un Gobierno y Gestión de TI que la apoye.

Ante la ausencia de un marco de referencia de un SGCS, las empresas o instituciones universitarias se ven en la tarea de trabajar en los planes de continuidad de negocio offline. Si logramos incluir una estrategia de continuidad de servicio de TI efectiva estaríamos aumentando la continuidad del negocio a través del servicio.

En esta investigación se analizará todo lo referente a la gestión de continuidad de servicios de TI y sus estándares asociados, desarrollando el caso de estudio aplicado a la Universidad del Norte; con el propósito de establecer un marco estratégico que permita a las universidades implementar un sistema de gestión de la continuidad del servicio de TI que apoye los servicios críticos del negocio de las instituciones universitarias en Colombia.

2. DESCRIPCIÓN DEL PROBLEMA

En Colombia son pocas las instituciones universitarias (IU) que actualmente tienen implementado un proceso de Gobierno y Gestión de TI que permita evaluar, orientar y supervisar los procesos de TI que apoyan los objetivos estratégicos, y que a su vez provea los lineamientos para la planificación, construcción, ejecución y control de la infraestructura tecnológica, que pueda garantizar la continuidad de los servicios de TI que soportan los procesos académicos, de investigación y extensión de la IU. Y que genere la capacidad operativa necesaria para minimizar el impacto en caso de que ocurra un desastre que los llegara afectar.

A pesar que en Colombia existen antecedentes de desastres naturales que impactaron la continuidad de los servicios en entidades educativas, como, por ejemplo, el caso de la ruptura del Jarillón de contención de las aguas del Río Bogotá en el año 2011, el cual inundó el 90% de la universidad de la sabana ocasionando indisponibilidad en los servicios, las instituciones universitarias en Colombia no implementan estrategias de continuidad puesto que la percepción de la probabilidad de ocurrencia no es alta y no cuenta con un gobierno y gestión de TI que apoye la estrategia, definiendo procesos, métricas, indicadores (BSC-SGSI and SGCS) y roles para su ejecución.

Otro factor influyente es la concepción que tienen las instituciones universitarias que manteniendo una estrategia de continuidad del negocio no requieren una estrategia de la continuidad de servicios TI. Lo cual es falso, ya que sus procesos Core se soportan también con tecnologías de información. Por lo cual, es importante minimizar interrupciones

inesperadas de sus servicios. Al igual que cualquier otro tipo de organización requieren entonces diseñar planes de continuidad de negocio orientados a la continuidad de sus activos tecnológicos, que les permitan salvaguardar la información crítica considerada el activo más valioso. Y les ayude a recuperarse en un tiempo aceptable para evitar la pérdida en la credibilidad de la institución y la indisponibilidad de la información.

Por otra parte, los cambios y la evolución de la tecnología están ocurriendo cada día a una velocidad más acelerada, ocasionando que para las instituciones universitarias sea más desafiante adaptarse y poder dar respuesta a los nuevos requerimientos de los usuarios. Lo cual se convierte en un reto mantener los niveles óptimos en la prestación de sus servicios ya que carecen de una estrategia de gestión óptima para alcanzar una exitosa continuidad en este.

3. JUSTIFICACIÓN

Para una institución universitaria privada en Colombia que dentro de sus ejes institucionales distintivos incluye el uso de la tecnología para la formación del estudiante, se le hace necesario contar con una estrategia de gestión de continuidad de servicios de TI, gestionado por un gobierno de TI que le permita mantener sus procesos Core operando de manera continua. Por consiguiente, en el caso que se presenten incidentes inesperados, esta estrategia de gestión de continuidad de servicios puede llegar a garantizar la pronta recuperación de los procesos y servicios de la institución universitaria, antes que la indisponibilidad de estos pueda provocar grandes pérdidas económicas, pérdida de imagen y/o credibilidad. La gestión de continuidad de servicios de TI se convierte entonces en uno de los soportes para la continuidad del negocio en la institución universitaria.

En este proyecto se busca establecer una revisión teórica y conceptual de SGCS, aplicados a las instituciones universitarias privadas en Colombia, los procedimientos existentes, los estándares más utilizados, con el propósito formular un modelo para soportar la estrategia del sistema SGCS, más adecuado para una institución universitaria.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un marco estratégico para gestionar la continuidad de los servicios de TI en Instituciones Universitarias Privadas Colombianas bajo la integración de buenas prácticas de gobierno y gestión TI caso de estudio: Universidad del Norte

4.2 OBJETIVO ESPECÍFICOS

1. Elaborar una revisión conceptual y referencial asociada con la gestión de continuidad de los servicios de TI.
2. Desarrollar una revisión conceptual y referencial de los estándares y asociada con la gestión de continuidad de los servicios de TI.
3. Elaborar un modelo conceptual que permita desplegar un marco estratégico de gestión de la continuidad del servicio de TI en Instituciones Universitarias.
4. Llevar a cabo un caso de estudio en la Universidad del Norte que facilite la implementación de un sistema de gestión de la continuidad del servicio de TI en Instituciones Universitarias.

5. METODOLOGÍA

5.1 TIPO DE INVESTIGACIÓN

La investigación que se desarrollará es de tipo Proyecto factible, la cual consiste en la investigación, elaboración y desarrollo de un modelo operativo viable para solucionar problemas, requerimientos necesidades de organizaciones o grupos sociales que pueden referirse a la formulación de políticas, programas, tecnologías, métodos, o procesos.

5.2 PERIODO Y LUGAR

Esta investigación se llevará a cabo en la Universidad del Norte en Barranquilla, entre los meses de febrero y mayo de 2018.

5.3 MÉTODO

Para esta investigación utilizaremos los métodos empíricos porque permiten la elaboración y obtención de los datos y el conocimiento de los hechos fundamentales que caracterizan a los fenómenos.

Los métodos empíricos utilizados serán:

- La observación
- La experimentación
- La entrevista.

5.4 ACTIVIDADES

a) Exploración de la situación actual de la universidad del norte entorno a la continuidad de los servicios de TI.

b) Revisión del estado del arte en otras instituciones de educación superior: se revisará si otras instituciones de educación superior cuentan con una estrategia para la continuidad de servicios de TI y en qué estándares se basaron.

c) Revisión de marcos de gobierno y gestión que apliquen para Universidades: Se estudiará los marcos líderes del mercado COBIT e ITIL para obtener las mejores prácticas posibles.

d) Realizar el diseño de la estrategia propuesto: se desarrollarán una serie de procesos que deben cumplir la organización cuando decida adoptar el diseño propuesto.

e) Elaborar el documento final: con la información recolectada y el análisis realizado se redactará el informe final.

f) Presentar propuesta: una vez finalizada la investigación se presentará ante los jurados académicos para su respectivo revisión y concepto. Adicionalmente los resultados se presentarán ante la Dirección de Tecnología Informática y de comunicaciones para determinar su viabilidad y aplicación a través de un plan de implementación del modelo para el SGCS.

6. ALCANCE

El alcance de este proyecto está enmarcado en el diseño de un marco estratégico para gestionar la continuidad de los servicios de TI en Instituciones Universitarias privadas en Colombia, bajo la integración de buenas prácticas del gobierno y gestión de TI. Soportado en el marco de trabajo de Cobit 5 y mejores prácticas de ITIL, que permitan llevar a cabo un caso de estudio en la Universidad del Norte que facilite la implementación de un sistema de gestión de la continuidad del servicio de TI en instituciones universitarias.

7. MARCO CONCEPTUAL

7.1 RESILIENCIA

Es la habilidad de adaptarse y recuperarse rápidamente de cualquier cambio en el ambiente conocido o desconocido a través de una implementación holística de manejo de riesgo, contingencia y plan de continuidad del negocio.[1]

7.1.1 Resiliencia operativa y continuidad de servicios de TI

La resiliencia operativa asociada a la continuidad de servicios de TI se puede definir como la capacidad que tiene una organización para recuperar su operación crítica durante los tiempos en que se producen eventos que amenazan su continuidad. Y la capacidad para adaptase y mejorar antes los cambios que se generan después de una situación adversa.

7.2 GOBIERNO CORPORATIVO

Con el fin de garantizar el cumplimiento de los requerimientos del negocio las compañías implementan un gobierno corporativo el cual consiste en el conjunto de relaciones entre la administración de la empresa, su consejo de administración, sus accionistas y otras partes interesadas. También proporciona la estructura a través de la que se fijan los objetivos de la compañía y se determinan los medios para alcanzar esos objetivos y supervisar el desempeño.[2]

[1] Swanson, Bowen, Phillips, Gallup, Lynes (2010) NIST Special Publication 800-34 Rev. 1 National Institute of Standards and Technology.
[2] Organización para la Cooperación y el Desarrollo Económicos, Principios de Gobierno Corporativo de la OECD, 2004

Otro concepto de gobierno corporativo es el que define Selig (2008) en su libro Implementing IT Governance, el cual se refiere al conjunto de responsabilidades y prácticas ejercidas por la Junta y la dirección ejecutiva, con el objetivo de proporcionar dirección estratégica, asegurando el cumplimiento de planes y objetivos, la gestión de los riesgos y asegurar el uso responsable de los recursos empresariales.

El gobierno corporativo se ocupa de la separación de la propiedad y el control de una organización, mientras que el gobierno empresarial se centra en la dirección y el control del negocio, y el gobierno de TI se centra en la dirección y el control de TI.

Tabla 1. Diferencias entre los gobiernos corporativo, empresarial y de TI en el contexto de la Universidades privadas.

Gobierno corporativo	**Gobierno Empresarial**	**Gobierno de TI**
Separación de propiedad y control	Dirección y control del negocio	Dirección y control de TI
• Roles del consejo directivo • Cumplimiento normativo y de leyes • Derechos del consejo directivo y del gobierno académico • Operaciones y Control de los procesos académicos, investigación y extensión • Contabilidad financiera e Informes • Gestión de riesgos	• Estrategia de negocios • Planes de desarrollo institucional • Procesos y actividades empresariales • Innovación e Investigación • Capital intelectual • Gestión de recursos humanos • Métricas de rendimiento y • controles • Gestión de activos	• Estrategia de TI, Planes y Objetivos • Alineación con planes de desarrollo institucional y objetivos • Recursos de TI • Gestión de la demanda • Entrega y Ejecución de Valor • Gestión proyectos • Administración de riesgo, cambio y rendimiento. • Gestión de la continuidad

Fuente: propia, adaptado de Selig G, Implementing IT Governance, 2008

7.3 GOBIERNO DE TI

Contempla aspectos como el marco legal y normativo, la estructura de TI, sus procesos, la gestión de relaciones y los acuerdos de servicio y desarrollo. Como producto del componente de Gobierno de TI se formalizan las:

- Políticas
- Estándares,
- Normas
- Lineamientos de TI.

El Gobierno de TI hace parte de los objetivos y las estrategias de las organizaciones, es por esto que es responsabilidad no solo de los gerentes o administradores de tecnología, los responsables de generar un ambiente correcto y de la aplicación de la misma; son los ejecutivos, directores, presidentes, es decir la alta gerencia administrativa junto con la gerencia de tecnología son los mayores responsables de generar el liderazgo, las estructuras, procesos y estrategias para que la organización lo implemente con éxito.[3]

Según Gad j Selig (2008) en su libro Implementing IT Governance el Gobierno, es el conjunto de procedimientos, estructuras y comportamientos utilizados para dirigir y controlar la organización hacía el logro de sus objetivos. A su vez establece un propósito y un alcance para el gobierno de TI.

[3] RAMÍREZ, G., CONSTAIN, G. Modelos y Estándares de Seguridad Informática. Palmira: UNAD. 2012. p. 50

7.3.1 Propósito del gobierno de TI - Gad j Selig (2008)

- Alinear las inversiones y prioridades de TI con las del negocio.
- Gestionar, evaluar, priorizar, financiar, medir y supervisar las solicitudes de servicios de TI, y los resultados, de una manera más consistente y repetible que optimice el valor del retorno al negocio.
- Mantener una utilización responsable de los recursos y activos.
- Definir claramente los roles y la autoridad en los procesos que competen a TI.
- Asegurar que TI cumpla con sus planes, presupuestos y compromisos.
- Gestionar los riesgos, amenazas, cambios y contingencias de forma proactiva.
- Mejorar el rendimiento de TI, el cumplimiento, la madurez, el desarrollo del personal y las iniciativas de outsoursing.
- Mejorar las relaciones y la satisfacción con los clientes
- Gestionar y pensar globalmente, pero actuar localmente.
- Favorece la innovación dentro de TI y el negocio.

7.3.2 Alcance del gobierno de TI - Gad j Selig (2008)

La estrategia clave de gobierno de TI y las decisiones de recursos deben abordar los siguientes temas:

(Modificado de Weill y Ross, 2004, Popper, 2000)

- Principios de TI: declaraciones de alto nivel sobre el uso de TI en el negocio (por ejemplo, escala, simplificación e integrar; Reducir el TCO (Costo Total de Operaciones) y el autofinanciamiento mediante la reinversión de ahorros; invertir en sistemas de cara a la comunidad; Transformar el negocio y la TI a través de la transformación de procesos empresariales; dirección del plan estratégico, PMO

(oficina de gestión de proyectos, mantener la innovación y cumplimiento normativo, etc.)

- Arquitectura de TI - lógica de organización de datos, aplicaciones e infraestructura capturada en un conjunto de políticas, relaciones, procesos, estándares y opciones técnicas, para lograr los negocios deseados e integración técnica y estandarización.

- Arquitectura SOA: la arquitectura orientada a servicios (SOA) es una arquitectura de TI que apoya la integración de la empresa como tareas vinculadas, repetibles o servicios; SOA ayuda a los usuarios a crear aplicaciones compuestas que se basan en la funcionalidad de múltiples fuentes dentro y fuera de la empresa para soportar procesos empresariales

- Infraestructura de TI: coordinada centralmente, basada en servicios de TI compartidos que son la base para la capacidad de TI y el soporte de la empresa.

- Inversión en TI y priorización: decisiones sobre cuánto y dónde invertir en IT (Por ejemplo, capital y gastos), incluidos proyectos de desarrollo y mantenimiento, infraestructura, seguridad, personas, etc.

- Desarrollo de personas (capital humano): decisiones sobre cómo desarrollar y mantener la sucesión en la gestión del liderazgo en TI y habilidades y competencias técnicas (dónde gastar en capacitación y desarrollo, industria individual y organizacional certificaciones, etc.)

- Políticas, procesos, mecanismos, herramientas y métricas de gobierno de TI: decisiones sobre composición y funciones de los grupos directivos, consejos asesores, técnicos y comités arquitectónicos, equipos de proyectos; Indicadores clave de rendimiento (KPI); Alternativas de contracargo; Informes de rendimiento, un proceso de auditoría significativo y la necesidad de contar con cada proyecto e inversión.

Un gobierno de TI exitoso se basa en tres pilares fundamentales:

1. Liderazgo, organización y toma correcta de decisión: define la estructura de la organización, roles, responsabilidades, derecho de decisión (influyente y responsable de la toma de decisiones), una visión compartida y una interfaz y/o puntos de contacto de integración. Este pilar asegura que:
    a. Los roles y las responsabilidades están bien definidos, incluyendo las jerarquías de dirección y revisión para la inversión, autorizaciones, resolución de cuestiones y exámenes periódicos formales.
    b. Existen contratos claros de transferencia y de interfaz y contratos para el trabajo interno y externo y entregable.
    c. Los líderes están motivados y tienen las competencias adecuadas.
    d. El CIO es un agente de cambio que vincula las TI al negocio.

2. Procesos flexibles y escalables: El modelo de gobierno de TI hace fuerte énfasis en la Importancia de la transformación y mejora del proceso: (por ejemplo, planificación, gestión de proyectos, gestión de inversiones de cartera, gestión de riesgos, gestión y

entrega de servicios de TI, Gestión del rendimiento, gestión de proveedores, controles y auditorías, etc.). Este pilar asegura que:

a. Los procesos están bien definidos, documentados y medidos.
b. Los procesos definen las interfaces entre las organizaciones y aseguran que el flujo de trabajo abarca los límites y silos incluyendo organización, vendedores, geografía, tecnología y cultura.
c. Los procesos son flexibles, escalables y aplicados consistentemente, con sentido común

3. Habilitación de tecnología: Corresponde a herramientas y tecnologías líderes que soportan las principales componentes del gobierno de TI. Este pilar asegura que:
    a. Los procesos son soportados por herramientas de software (Por ejemplo, planificación y presupuestación, gestión de la inversión de cartera, gestión de proyectos, gestión de cambios, gestión de servicios de TI y procesos de entrega, financiera, activa.
    b. Las herramientas proporcionan indicadores de gobierno, comunicaciones y eficacia para acelerar las decisiones, acciones de seguimiento y gestión.

7.4 FRAMEWORK INTEGRADO DE TI

Gad j Selig (2008) establece que el marco de gobierno integrado se conforma de cinco componentes críticos de TI basados en un estudio de mejores prácticas de la industria y abordan las siguientes áreas de trabajo:

- Estrategia de negocio, el plan y los objetivos (gestión de la demanda): esto implica el desarrollo de la estrategia y el plan de negocio que deben impulsar la estrategia y el plan de TI.

- Estrategia de TI, plan y objetivos (gestión de la demanda): esto debe basarse en la plan de negocios y objetivos, y proporcionará la dirección y las prioridades de las funciones de TI y recursos; Inversiones de cartera, prioridad e identificar los derechos de decisión (quién influye en las decisiones y quién está autorizado para tomar las decisiones) en una amplia variedad de áreas de TI; Además, el CIO es responsable de las inversiones en infraestructura tales como servidores, redes, software de administración.

- Ejecución del plan de TI (gestión de la ejecución): abarca los procesos de gestión de proyectos y gestión de servicios de TI (incluyendo ITIL – Infraestructura IT), Gestión de riesgos y amenazas, gestión del cambio, seguridad, planes de contingencia y otros.

- Gestión del rendimiento y controles de gestión: incluye áreas tales como el Balanced Scorecard, indicadores clave de desempeño, COBIT y áreas de cumplimiento regulativo.

- Gestión de proveedores y gestión de outsourcing (gestión de la ejecución): las empresas están incrementando su gasto de outsourcing, seleccionando y administrando los proveedores y sus entregables se han vuelto críticos.

- El desarrollo de las personas, la mejora continua del proceso y el aprendizaje: invertir en las personas, la gestión del conocimiento y sostener la mejora continua iniciativas de innovación.

Para cada componente de gobierno de TI, el primer paso para un nuevo CIO es evaluar el medio ambiente y la forma en la que se encuentra. La figura 1 muestra el Framework integrado de TI.

Tabla 2. Marco de Gobierno de TI integrado

Areas of Work	Description/Components	Deliverables/References
Business Plan/ Objectives (Demand Management & Alignment)	• Strategic Business Plan – Vision, Objectives, Financials, Operations, SWOT, Imperatives (Must Do's), Initiatives (Alternatives that Support Imperatives), etc. • Capital Planning/Expense Planning & Budgeting • Business Performance Management (Key Metrics) • Executive and Other Steering & Review Councils; Organization Structure	• Plan Document • Financials • Balanced Scorecard Metrics • BCG; Porter; Hamel
IT Plan, Objectives, Portfolio Investment and Approvals (Demand Management & Alignment)	• IT Plan is aligned with the Business Plan – IT Capital/Expense Budget • IT portfolio investment, rationalization, selection, prioritization, funding and approval (Portfolio Management Model (for New, Change Programs and Projects and/or Operational initiatives and Infrastructure Functions) • Fund major Initiatives • IT Performance Management (Define Metrics and Measurement Criteria)	• IT Strategic/Tactical Plan/ Metrics • Portfolio Mgt. Model (Investment Criteria); ITIM • Engagement Model - Roles • Business Rules & Authorization • McFarlan, Cash; Luftman; Popper; Selig
IT Plan Execution & Delivery (Resource & Execution Management)	• Program, Project and Operating Plans (Capital Plans, Project Plans and Budgets) • Policies, Standards, Guidelines & Processes (e.g. Management Control, Enterprise Architecture, Security, PMO, ITIL, Enterprise Architecture, etc.) • Processes (PMO, Help Desk, Security, Administrative SOPs, Workflows, Change, Risk, etc.) • Financial, program, project, application, maintenance and operational accountability	• Assess Implications of PMMM, PMBOK, CMMI, ITIL, SDLC, CoBit, Security (ISO 17799), Prince2 ,eSCM Frameworks • Infrastructure & Operational Integrity, Continuity & Security
Performance Management, Controls, Risk, Compliance and Vendor Management (Execution Management)	• Manage and measure plans, budgets programs, projects, operations & risks • Define and track key performance indicators (KPI) • Compare plans to actuals and take appropriate corrective actions • Outsourcing and Vendor Selection, Tracking, Measurement • Business and IT Continuity, Security Contingency and Disaster Recovery	• Balanced Scorecard & KPIs • Performance Management • RFI, RFQ, RFP and Contrac Management; • Sarbanes-Oxley ++ Compliance • Management Controls/ COBIT
People Development, Continuous Process Improvement & Learning	• Human capital development • Organizational, Project & Operational Maturity Models and Standards • Managing Change and Transformation (e.g. culture, interoperability) • Training and Certification (e.g. Individual and Organization)	• Adopt Current and Emerging Industry and Government Best Practices Standards & Guidelines • PCMM; ITSM; ISO; ITIM • Career Development and Certification

Fuente: Selig, G, Implementing IT Governance, (2008)

7.5 ESTRATEGIA DE TI

Este dominio tiene el fin de apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las instituciones, para lograr que esté alineada con las estrategias organizacionales y sectoriales.

El modelo de gestión debe permitir el despliegue de una estrategia de TIC que garantice la generación de valor estratégico de la capacidad y la inversión en tecnología. Al componente de Estrategia de TI le llegan como insumo la estrategia organizacional y las necesidades del negocio.

7.6 SISTEMA DE GESTIÓN

Es el conjunto de políticas, procesos y procedimientos utilizados por una organización con el fin de garantizar el cumplimiento de las tareas necesarias para alcanzarlos los objetivos de la misma. La mayoría de los sistemas de gestión están basados en el círculo de Deming.

7.6.1 Círculo de Deming:

El ciclo PDCA (o círculo de Shewhart) (Ver Figura 1.), es el sistema más usado para implantar un sistema de mejora continua cuyo principal objetivo es la auto-evaluación, destacando los puntos fuertes que hay que tratar de mantener y las áreas de mejora en las que se deberá actuar.

Figura 1. Ciclo de mejora continúa

Fuente: http://equipo.altran.es/el-ciclo-de-deming-la-gestion-y-mejora-de-procesos/

El ciclo PDCA de mejora continua está conformado por cuatros etapas cíclicas, es decir, una vez que termina la etapa final, se vuelve nuevamente a la etapa inicial e inicia nuevamente el ciclo.

Las cuatro etapas cíclicas son:

- Plan (planificar): Se identifica las actividades que son susceptibles de mejora, se definen objetivos, se generan indicadores de control y se establecen las herramientas para el logro de los objetivos.
- Do (Hacer): Se ejecuta el plan de acción, teniendo en cuenta las tareas planificadas, se controla el plan y su verificación y se obtiene retroalimentación para un posterior análisis.
- Check (Verificar): Se comprueba los logros obtenidos después de implementada la mejora en relación a las metas u objetivos que se establecieron en la fase inicial. Esta

verificación se realiza a través de indicadores, diagrama de paretos o una lista de chequeo.

- Act (Actuar): Después de establecer el resultado obtenido, es el momento de definir acciones correctivas y preventivas que permitan mejorar los puntos que lo requieran, así como consolidar las metodologías efectivas.

8. MARCO REFERENCIAL

Los marcos de referencia conocidos tienden a atacar los problemas de continuidad utilizando la continuidad de negocio, actualmente no existe dentro de los modelos revisados una estrategia de continuidad del servicio que contemple resiliencia a nivel de servicio. Propondremos una estrategia para la continuidad de servicio que integraremos a un modelo de gobierno con el fin de establecer los roles, indicadores y métricas de gestión. Por lo anterior tendremos como referencia COBIT 5, ITIL V3, e ISO 9001:2015.

8.1 COBIT

8.1.1 Introducción marco de Cobit

Cobit (Objetivos de control para la información y tecnologías relacionadas), es una guía de buenas prácticas que están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones facilitadas por la TI, asegurará la entrega del servicio y brindarán un patrón de medición con el cual se podrá calificar cuando las cosas no vayan bien. Para que la TI tenga éxito en satisfacer los requerimientos del negocio, la dirección empresarial debe implantar un sistema de control interno o un marco de trabajo. El marco de trabajo de Cobit es mantenido por ISACA (en inglés: Information Systems Audit and Control Association) y el IT GI (en inglés: IT Governance Institute).

8.1.2 Cobit 5

COBIT5 proporciona un marco integral que ayuda a las Organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de la TI de la Organización.[4]

Los principios y habilitadores de Cobit 5 son genéricos y pueden ser aplicados a cualquier tipo de empresa, sin importar el tamaño o el sector al que pertenezca. Puede aplicarse a:

- La seguridad de la información
- La gestión del riesgo
- El gobierno corporativo y la gestión de las TI de la empresa
- Las actividades de revisión y garantía
- La conformidad legal y regulatoria
- El tratamiento de datos financieros o de información sobre Responsabilidad Social Corporativa.

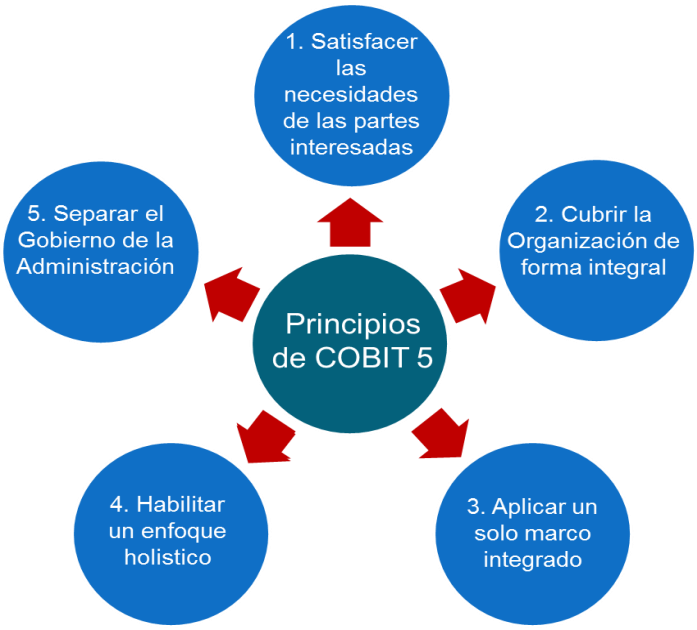
8.1.3 Principios de Cobit 5

Cobit 5 une los cinco principios: Satisfacer las necesidades de las Partes Interesadas, Cubrir la organización de Forma Integral, Aplicar un solo Marco Integrado, Habilitar un Enfoque Holístico y Separar el Gobierno de la Administración que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie holística de

[4] https://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. (Ver Figura 2.)

Figura 2. Principios de Cobit 5



Fuente: COBIT5-Introduction-Spanis ISACA

8.1.4 Procesos de gobierno y gestión

Cobit 5 establece claramente una distinción entre gobierno y gestión, estas dos disciplinas contemplan diferentes tipos de actividades, diferentes estructuras organizacionales y diferentes propósitos.

8.1.4.1 Proceso de Gobierno

Garantiza que se evalúen las necesidades de las partes interesadas, para establecer los objetivos corporativos que se quieren lograr; se establecen prioridades y se toman decisiones; y se supervisa la salida (Evaluar, orientar y supervisar [EDM].

Este dominio está conformado por cinco procesos de gobierno en donde se definen prácticas de evaluación, dirección y supervisión.

Tabla 3. Procesos de Gobierno

Código	Descripción
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno
EDM02	Asegurar la entrega de beneficios
EDM03	Asegurar la optimización del riesgo
EDM04	Asegurar la optimización de recursos
EDM05	Asegurar la transparencia hacia las partes interesadas

Fuente: COBIT5

8.1.4.2 Proceso de Gestión

La gestión planifica (APO), construye (BAI), opera (DSS) y monitorea (MEA) las actividades establecidas por el gobierno para lograr los objetivos de la organización.

Este dominio está conformado las siguientes prácticas:

- Alinear, Planear y Organizar - APO

Tabla 4. Proceso de Gestión - APO

Código	Descripción
APO01	Gestionar el marco de gestión de ti
APO02	Gestionar la estrategia
APO03	Gestionar la arquitectura empresarial

APO04	Gestionar la innovación
APO05	Gestionar el portafolio
APO06	Gestionar el presupuesto y los costos
APO07	Gestionar los recursos humanos
APO08	Gestionar las relaciones
APO09	Gestionar los acuerdos de servicio
APO10	Gestionar los proveedores
APO11	Gestionar la calidad
APO12	Gestionar el riesgo

Fuente: COBIT5

- Construir, Adquirir e Implementar - BAI

Tabla 5. Proceso de gestión - BAI

Código	Descripción
BAI01	Gestión de programas y proyectos
BAI02	Gestionar la definición de requisitos
BAI03	Gestionar la identificación y construcción de soluciones
BAI04	Gestionar la disponibilidad y la capacidad
BAI05	Gestionar la facilitación del cambio organizativo
BAI06	Gestionar los cambios
BAI07	Gestionar la aceptación del cambio y la transición
BAI08	Gestionar el conocimiento
BAI09	Gestionar los activos
BAI10	Gestionar la configuración

Fuente: COBIT5

- Entregar, Servir y Dar Soporte – DDS

Tabla 6. Proceso de gestión - DSS

Código	Descripción
DSS01	Gestionar Operaciones
DSS02	Gestionar Peticiones e Incidentes de Servicio

DSS03	Gestionar Problemas
DSS04	Gestionar la Continuidad
DSS05	Gestionar Servicios de Seguridad
DSS06	Gestionar Controles de Proceso de Negocio

Fuente: COBIT5

- Monitorear, Evaluar y Valorar – MEA

Tabla 7. Proceso de gestión - MEA

Código	Descripción
MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad
MEA02	Supervisar, evaluar y valorar el sistema de control interno
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

Fuente: COBIT5

A continuación se muestran los 37 objetivos de control, agrupados en cinco dominios agrupados. Ver Figura 3.

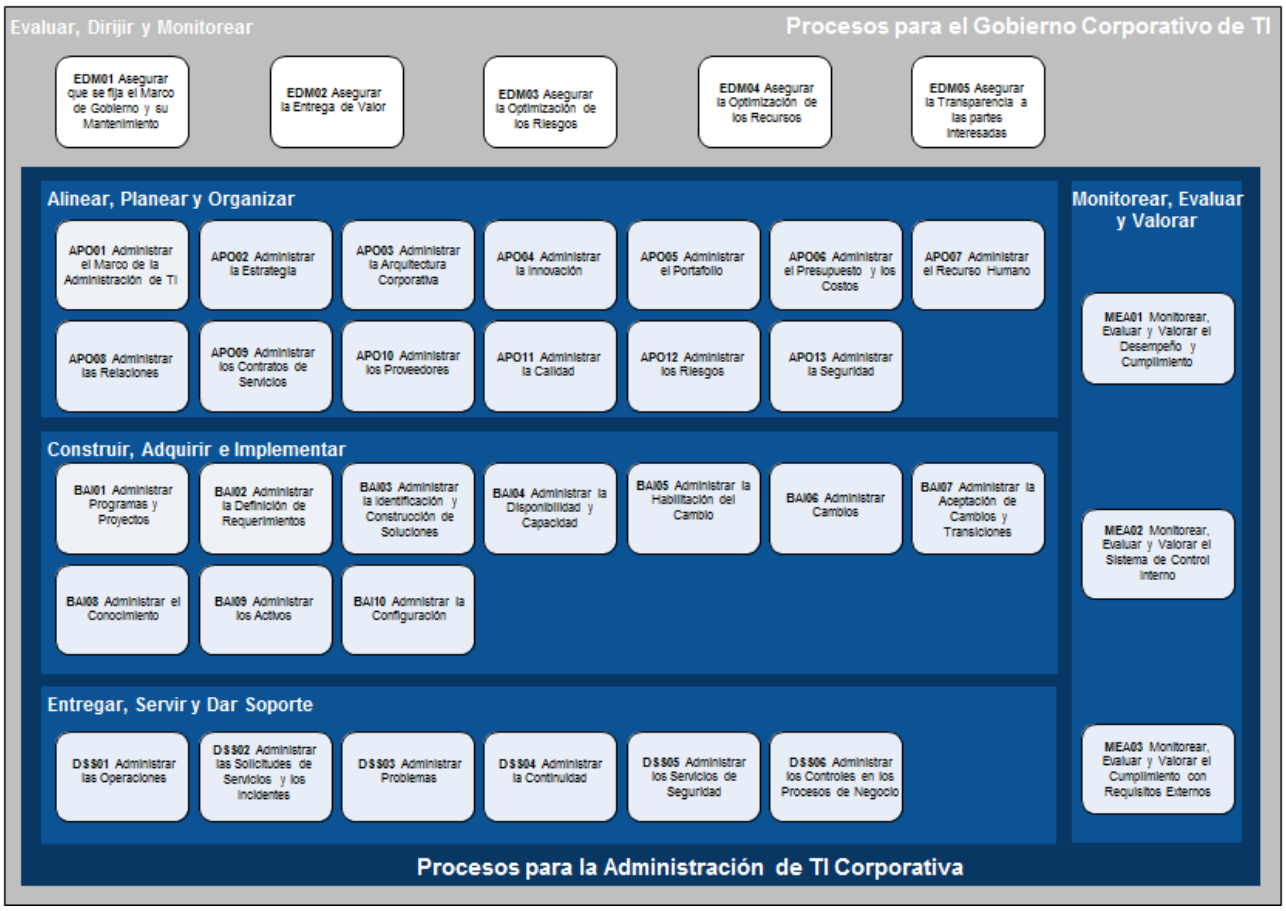


Figura 3. Procesos de Gobierno y Gestión de TI de Cobit 5

Fuente: COBIT5-Introduction-Spanis ISACA

8.2 ITIL

Es el conjunto de conceptos y mejores prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL describe detalladamente un extenso conjunto de procedimientos de gestión que ayudan a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

ITILV3 está estructurado por 5 libros que consolidan el ciclo de vida del servicio: Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio. Ver Figura 4.

Figura 4. Ciclo de vida del servicio[5]

8.2.1 Estrategia del servicio

Provee una guía en el cómo diseñar, desarrollar e implementar la Gestión de Servicios, no solo como una capacidad organizacional sino como un activo estratégico.

Se encarga de fijar objetivos, políticas y lineamientos para la gestión de servicios.

Las actividades de la Estrategia de Servicios son:

- Definir el mercado
- Desarrollar las ofertas
- Desarrollar los activos estratégicos

[5] Fuente: https://www.servicetonic.es/itil/introduccion-a-itil-v3/

- Preparar la ejecución

Los procesos de la Estrategia del servicio son:

- Gestión del portafolio de servicios o cartera de servicios
- Gestión de la demanda
- Gestión financiera

8.2.2 Diseño del servicio

Provee una guía para el diseño y desarrollo de servicios y los procesos de gestión del servicio. Entre sus principales metas y objetivos se encuentra el diseñar servicios que puedan ser fácilmente y eficientemente desarrollados y mejorados, identificar y gestionar riesgos y ofrecer un enfoque principalmente en las personas, los procesos, los productos y los socios de negocio.

Los procesos del Diseño de servicio son:

- Gestión de los niveles de servicio
- Gestión del catálogo de servicios
- Gestión de la disponibilidad
- Gestión de la seguridad de la información
- Gestión de proveedores
- Gestión de la capacidad
- Gestión de continuidad de servicios de TI

8.2.3 Transición del servicio

Provee una guía en el desarrollo y mejora de las capacidades para transicionar servicios nuevos y modificados a operaciones. Su principal objetivo es trasladar a producción controlando el riesgo de falla los requerimientos establecidos en la estrategia del servicio y diseñados por el diseño de servicio.

Los procesos de la transición del servicio son:

- Planeamiento y soporte de la transición
- Gestión del cambio
- Gestión de la configuración y Activos del servicio
- Gestión de implementación y versiones
- Validación del servicio y prueba
- Evaluación
- Gestión del conocimiento

8.2.4 Operación del servicio

Provee una guía para obtener eficiencia y efectividad en la entrega y soporte de los servicios, para asegurar valor al cliente y para el proveedor del servicio. El propósito de la operación del servicio es coordinar y realizar actividades y procesos requeridos para entregar y gestionar los servicios a los clientes y usuarios a los niveles acordados.

Los procesos de operación del servicio son:

- Gestión de eventos
- Gestión de incidencias
- Gestión de peticiones de servicio

- Gestión de problemas
- Gestión de acceso

Las funciones asociadas a la operación del servicio son:

- Service Desk
- Gestión técnica
- Gestión de operaciones de TI
- Gestión de aplicaciones

8.2.5 Mejora continua del servicio

Es una guía instrumental de la creación y mantenimiento del valor. El propósito es alinear y realinear los servicios con las necesidades cambiantes de negocio identificando e implementando mejoras.

Los procesos asociados a la mejora continua del servicio son:

- Definir lo que se debería medir
- Definir lo que podemos medir
- Recopilar datos
- Procesar los datos
- Analizar los datos
- Presentar y usar la información
- Implementar acciones correctivas

8.3 CONTINUIDAD DEL NEGOCIO

Es uno de los principales mecanismos de defensa para el negocio ante los desastres se define como, la capacidad estratégica y táctica de una organización de planear y responder a los incidentes e interrupciones del negocio con el fin de continuar las operaciones en un término aceptable. (BC standard, BSI 25999) [Traducción del autor].

8.4 GESTIÓN DE LA CONTINUIDAD DE LAS TIC

Estándar para alinear la continuidad del Servicio de las TIC con la Continuidad del Negocio (BSI 25999). Define un código de buenas prácticas sobre continuidad centrado en las infraestructuras TIC de las organizaciones, teniendo en cuenta que en la actualidad una gran parte de la continuidad del negocio de muchas organizaciones se basa en la continuidad de sus infraestructuras TIC. (BS 25777:2008)

8.5 GESTIÓN DE LA CONTINUIDAD DEL SERVICIO DE TI (ITSCM)

La Gestión de la Continuidad del Servicio de TI (IT Service Continuity Management, ITSCM) se ocupa de que el proveedor de servicios de TI siempre pueda proveer un mínimo nivel del servicio propuesto reduciendo el riesgo de eventos desastrosos hasta niveles aceptables y planificando la recuperación de servicios de TI. La ITSCM debe diseñarse para que apoye la gestión de la continuidad del negocio.

9. MODELO PROPUESTO

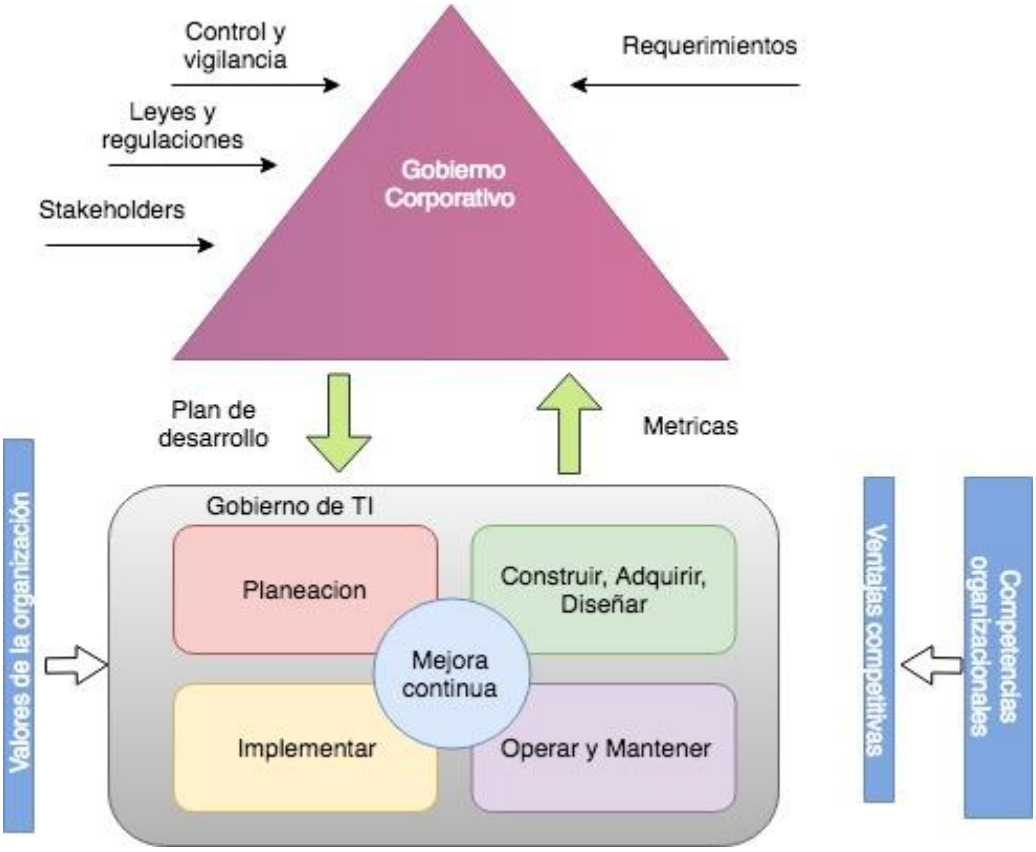


Figura 5. Marco estratégico de gestión para la continuidad de los servicios de TI en instituciones universitarias privadas en Colombia

9.1 DESCRIPCIÓN DEL MODELO

El modelo propone contar con un Gobierno y Gestión de TI que permita establecer un marco estratégico para la continuidad de los servicios de TI en instituciones universitarias privadas en Colombia apalancado en ITIL y Cobit 5.

El modelo contempla un gobierno corporativo que se encarga del control y vigilancia enmarcado en el ciclo de mejora continua.

Tabla 8. MEGCS

Marco estratégico de gestión para la continuidad de los servicios de TI (MEGCS)							
Planeación		**Construir, Adquirir y Diseñar**		**Implementar**		**Operar**	
Referencia	Proceso	Referencia	Proceso	Referencia	Proceso	Referencia	Proceso
COBIT APO01	Gestionar el Marco de Gestión de TI	COBIT BAI02	Gestionar la Definición de Requisitos	COBIT BAI01	Gestionar los Programas y Proyectos	COBIT DSS01	Gestionar las Operaciones
COBIT APO02	Gestionar la Estrategia	COBIT BAI03	Gestionar la Identificación y la Construcción de Soluciones	COBIT BAI06	Gestionar los Cambios	COBIT DSS02	Gestionar las Peticiones y los Incidentes del Servicio
COBIT APO09	Gestionar los Acuerdos de Servicio	COBIT MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	COBIT BAI10	Gestionar la Configuración	COBIT DSS04	Gestionar la Continuidad
COBIT APO12	Gestionar el Riesgo	ITIL02	Diseño del Servicio	ITIL03	Transición del Servicio	COBIT BAI04	Gestionar la Disponibilidad y la Capacidad
COBIT APO13	Gestionar la Seguridad					ITIL04	Operación del Servicio
ITIL01	Estrategia del Servicio						

9.1.1 Planeación

9.1.1.1 Gestionar el Marco de Gestión de TI

Descripción: Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso

de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.

Prácticas:

- Definir el alcance, las funciones internas y externas, los roles internos y externos, y las capacidades y los derechos de decisión requeridos, incluidas actividades de TI realizadas por terceras partes.
- Establecer un Comité Estratégico de TI (o equivalente) a nivel del Consejo de Administración.
- Contribuir al proceso de continuidad del servicio de TI manteniendo actualizada la información de contacto y las descripciones de roles de la empresa.

9.1.1.2 Gestionar la Estrategia

Descripción: Proporcionar una visión holística del negocio actual y del entorno de TI y la dirección futura, manteniendo o aumentando los niveles de continuidad de servicio.

Prácticas:

- Definir las iniciativas necesarias para cerrar las diferencias y migrar del entorno actual al deseado, incluyendo el presupuesto de inversión/operativo, fuentes de financiación y estrategia de provisión.
- Desarrollar y mantener una red de aprobación, apoyo e impulso de la estrategia de TI.
- Desarrollar un plan de comunicación que cubra los mensajes necesarios, audiencias objetivo, mecanismos/canales de comunicación y horarios.

9.1.1.3 Gestionar los Acuerdos de Servicio

Descripción: Alinear los servicios de TI y los niveles de servicio con las necesidades y expectativas de la empresa.

Prácticas:

- Valorar los servicios TI actuales y los niveles de servicio para identificar lagunas entre los servicios existentes y los procesos de negocio de los que son base. Identificar áreas de mejora de los servicios existentes y de las opciones de nivel del servicio.
- Analizar, estudiar y estimar la futura demanda y confirmar la capacidad de los servicios TI existentes.
- Analizar los requisitos para acuerdos de servicios nuevos o modificados recibidos desde la gestión de las relaciones con el negocio para asegurar que los requisitos puedan ser emparejados con los niveles de servicio. Considerar aspectos tales como tiempos del servicio, disponibilidad, rendimiento, capacidad, seguridad, continuidad, cumplimiento normativo y regulatorio, usabilidad y limitaciones de la demanda.
- Mantener una relación estrecha con la gestión de proveedores para asegurar que los contratos comerciales apropiados con proveedores de servicio externos cimientan los acuerdos de servicio con los clientes, siempre que sea aplicable.
- Establecer y mantener medidas para supervisar y recolectar datos del nivel del servicio.
- Hacer revisiones regulares para anticipar e identificar tendencias en el rendimiento del nivel de servicio.

9.1.1.4 Gestionar el Riesgo

Descripción: Identificar, evaluar y reducir los riesgos de TI relacionados con la continuidad del servicio de forma continua, dentro de niveles de tolerancia establecidos por la organización.

Prácticas:

- Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.
- Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.
- Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.
- Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.

9.1.1.5 Gestionar la Seguridad

Descripción: Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

Prácticas:

- Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.
- Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.

9.1.2 Construir, Adquirir y Diseñar

9.1.2.1 Gestionar la Definición de Requisitos

Descripción: Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios.

Prácticas:

- Definir e implementar la definición de requerimientos y el procedimiento de mantenimiento y un repositorio de requisitos acorde al tamaño, complejidad, objetivos y riesgos de la iniciativa que la empresa está considerando acometer. Expresar los requerimientos de la empresa en términos de cómo la diferencia entre las capacidades de negocio existente y deseadas son tratadas y como cada rol interactuará con la solución y la utilizará.
- Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados, obtenidos, priorizados y registrados de un modo comprensible para las partes interesadas, patrocinadores de negocio y personal de la implementación

técnica, reconociendo que los requerimientos pueden cambiar y llegar a ser más detallados según se implementen.

- Especificar y priorizar la información, los requerimientos técnicos y funcionales basados en los requerimientos de las partes interesadas. Incluir requerimientos de control de la información en los procesos de negocio, procesos automatizados y entornos de TI para hacer frente a los riesgos de la información y cumplimiento con regulaciones, leyes y contratos comerciales.
- Validar todos los requerimientos mediante aproximaciones tales como revisión por iguales, validación del modelo o prototipo operativo

9.1.2.2 Gestionar la Identificación y la Construcción de Soluciones

Descripción: Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.

Prácticas:

- Diseñar la redundancia, recuperación y copia de seguridad apropiadas.
- Considerar el impacto de las necesidades de la solución en el rendimiento de la infraestructura, considerando el número de activos informáticos, intensidad de ancho de banda y tiempo en que la información se considera sensible.

- Considerar cuando el efecto de las personalizaciones y las configuraciones acumuladas (incluyendo cambios menores que no estaban sujetos a unas especificaciones de diseño formal) requieran una revalidación a alto nivel de la solución y funcionalidad asociada
- Configurar que el software de aplicación adquirido cumple con los requerimientos de proceso de negocio.
- Crear un plan de pruebas integradas y prácticas acordes al entorno de la empresa y planes estratégicos de tecnología que catalizarán la realización de pruebas apropiadas en entornos de simulación para ayudar a verificar que la solución estará operativa satisfactoriamente en el entorno real y entregar los resultados esperados y que los controles son adecuados.
- Crear un entorno de pruebas que soporte el alcance completo de la solución y refleje, lo más fielmente posible, las condiciones del mundo real, incluyendo los procesos y procedimientos de negocio, rango de usuarios, tipos de transacciones y condiciones de desarrollo.

9.1.2.3 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

Descripción: Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.

Prácticas:

- Identificar requisitos externos de cumplimiento.
- Optimizar la respuesta a requisitos externos.
- Confirmar el cumplimiento de requisitos externos.
- Obtener garantía de cumplimiento de requisitos externos.

9.1.3 Implementar

9.1.3.1 Gestionar los Programas y Proyectos

Descripción: Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.

Prácticas:

- Actualizar el enfoque de gestión de programas y proyectos sobre la base de las lecciones aprendidas en su uso.
- Mantener el plan del proyecto y cualquier plan dependiente (por ejemplo, plan de riesgo, plan de calidad, plan de obtención de beneficios) para asegurar que están actualizados y reflejan su progreso real y los cambios materiales aprobados.
- Proporcionar garantías de calidad para los entregables del proyecto, identificar a propietarios y responsabilidades, revisar el proceso de calidad, criterios de éxito y las métricas de desempeño.
- Reevaluar el riesgo del proyecto periódicamente, incluyendo al inicio de cada fase de un proyecto importante y como parte de las evaluaciones de solicitudes de cambios importantes.

- Medir el rendimiento del proyecto versus criterios claves de rendimiento. Analizar las desviaciones de criterios claves de desempeño por su causa y evaluar los efectos positivos y negativos en el programa y los proyectos que lo componen.
- Recomendar y supervisar las acciones correctivas, cuando sean requeridas, en línea con el marco de gobierno de programas y proyectos.

9.1.3.2 Gestionar los Cambios

Descripción: Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.

Prácticas:

- Utilizar peticiones de cambio formales para posibilitar que los propietarios de procesos de negocio y TI soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones. Asegurar que todos estos cambios surgen solo a través del proceso de gestión de las peticiones de cambio.
- Categorizar todas las peticiones de cambio (ej. procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software externo adquirido) y relacionarlas con los elementos de configuración afectados.
- Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio.

- Planificar y programar todos los cambios aprobados.
- Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.
- Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se ha aplicado el cambio.
- Supervisar todos los cambios de emergencia y realizar revisiones post-implantación involucrando a todas las partes interesadas. La revisión debería considerar e iniciar acciones correctivas basadas en causas raíz tales como problemas en los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales e integridad de datos.
- Definir qué constituye un cambio de emergencia.
- Categorizar las peticiones de cambio en el proceso de seguimiento (ej. rechazados, aprobados pero aún no iniciados, aprobados y en proceso y cerrados).
- Mantener un sistema de seguimiento e informe para todas las peticiones de cambio.

9.1.3.3 Gestionar la Configuración

Descripción: Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

Prácticas:

- Definir y acordar el alcance y nivel de detalle para la gestión de la configuración (p.ej., qué servicios, activos y elementos configurables de la infraestructura se incluyen).
- Establecer y mantener un modelo lógico para la gestión de la configuración, incluyendo información sobre los tipos de elementos de configuración, atributos de los elementos de configuración, tipos de relaciones, atributos de relación y códigos de estado.
- Revisar los cambios propuestos a los elementos de configuración respecto a la base de referencia para garantizar su integridad y precisión.
- Verificar periódicamente los elementos de configuración en activo contra el repositorio de configuración comparando configuraciones físicas y lógicas, usando las herramientas apropiadas de descubrimiento, según sea necesario.
- Informar y revisar todas las desviaciones de las correcciones o acciones aprobadas para eliminar los activos no autorizados.
- Establecer y revisar periódicamente el objetivo de completitud del repositorio de configuración basado en las necesidades del negocio.

9.1.4 Operar

9.1.4.1 Gestionar las Operaciones

Descripción: Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de

procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

Prácticas:

- Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.
- Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento (throughput) de las actividades programadas.
- Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.
- Identificar y mantener una lista de activos de infraestructura que necesiten ser monitorizados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.
- Definir e implantar reglas que identifiquen y registren violaciones de umbral y condiciones de eventos. Encontrar un equilibrio entre la generación de eventos falsos menores y eventos significativos, de forma tal que los registros de eventos no estén sobrecargados con información innecesaria.
- Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.

9.1.4.2 Gestionar las Peticiones y los Incidentes del Servicio

Descripción: Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y

completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.

Prácticas:

- Definir esquemas de clasificación y priorización de incidentes y peticiones de servicio y criterios para el registro de problemas, para asegurar enfoques consistentes en el tratamiento, informando a los usuarios y realizando análisis de tendencias.
- Definir reglas y procedimientos de escalamiento de incidentes, especialmente para incidentes importantes e incidentes de seguridad.
- Para posibilitar análisis de tendencias, clasificar incidentes y peticiones de servicio identificando tipo y categoría.
- Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Hacer referencia a los recursos de conocimiento disponibles (incluyendo errores y problemas conocidos) para identificar posibles resoluciones de incidentes (soluciones temporales y/o soluciones permanentes).
- Ejecutar acciones de recuperación, si se requieren.

9.1.4.3 Gestionar la Continuidad

Descripción: Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

Prácticas:

- Identificar las partes interesadas clave y los roles y responsabilidades para definir y acordar la política de continuidad y su alcance.
- Identificar procesos de soporte al negocio esenciales y servicios TI relacionados.
- Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas.
- Definir los objetivos para ejercitar y probar los sistemas del plan.
- Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.
- Realizar un análisis y revisión post-ejercicio para considerar el logro.
- Desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de la revisión.
- Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales, tanto estratégicos como operativos.
- Recomendar y comunicar los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades.
- Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes.
- Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.
- Supervisar habilidades y competencias basándose en los resultados de los ejercicios y las pruebas.
- Gestionar acuerdos de respaldo.
- Evaluar la observancia del Plan de Continuidad de Negocio (BCP) documentado.

- Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, infraestructura técnica y estructuras organizativas y relaciones.

9.1.4.4 Gestionar la Disponibilidad y la Capacidad

Descripción: Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.

Prácticas:

- Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.
- Planificar requisitos de servicio nuevo o modificado.
- Supervisar y revisar la disponibilidad y la capacidad.
- Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.

9.2 MÉTRICAS

En la siguiente tabla se encuentran las métricas establecidas por el marco estratégico de gestión para la continuidad de los servicios de TI:

Tabla 9.Métricas

Proceso	Métrica
Gestionar el Marco de Gestión de TI	Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI
	Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costos
Gestionar la Estrategia	Porcentaje de objetivos en la estrategia de TI que soportan la estrategia de negocio
	Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos
Gestionar los Acuerdos de Servicio	Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
	Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información
Gestionar el Riesgo	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
	Frecuencia de actualización del perfil de riesgo
Gestionar la Seguridad	Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública
	Número de servicios de TI con los requisitos de seguridad pendientes
	Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados
	Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
Gestionar los Programas y Proyectos	Número de programas/proyectos ejecutados en plazo y en presupuesto
	Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
Gestionar la Definición de Requisitos	Porcentaje de requerimientos repetidos debido a la no alineación entre las necesidades y expectativas de la organización
	Nivel de satisfacción de las partes interesadas con los requerimientos
Gestionar la Identificación y la Construcción de Soluciones	Número de errores encontrados durante las pruebas
	Tiempo y esfuerzo para completar las pruebas
Gestionar la Disponibilidad y la Capacidad	Número de interrupciones del negocio debidas a incidentes en el servicio de TI
	Número de actualizaciones de capacidad, rendimiento o disponibilidad no planificada

	Número de picos de transacciones donde se excede la meta de rendimiento
	Número de incidentes de disponibilidad
	Número de eventos donde la capacidad ha excedido los límites planificados
Gestionar los Cambios	Porcentaje sobre el total de cambios que corresponde a cambios de emergencia
	Número de cambios de emergencia no autorizados una vez hecho el cambio
	Reducción en el tiempo y esfuerzo necesarios para aplicar los cambios
Gestionar la Configuración	Número de desviaciones ente el repositorio de configuración y la configuración real
	Número de discrepancias relativas a información de configuración incompleta o inexistente
Gestionar las Operaciones	Número de procedimientos operativos no estándar ejecutados
	Número de incidentes causados por problemas operativos
Gestionar las Peticiones y los Incidentes del Servicio	Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio
	Porcentaje de incidentes resueltos dentro de un periodo acordado/ aceptable
	Nivel de satisfacción del usuario con la resolución de las peticiones de servicio
	Tiempo promedio transcurrido para el tratamiento de cada tipo de petición de servicio
Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	Tiempo medio transcurrido entre la identificación de los problemas de incumplimiento y su resolución
	Frecuencia de revisiones de cumplimiento
Gestionar la Continuidad	Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento
	Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo
	Porcentaje de medios de respaldo transferidos y almacenados de forma segura
	Número de sistemas críticos para el negocio no cubiertos por el plan
	Número de ejercicios y pruebas que han conseguido los objetivos de recuperación
	Frecuencia de las pruebas

9.3 ROLES

Con el fin de soportar el modelo propuesto se especifican los siguientes roles, que apoyaran las actividades descritas anteriormente:

- Director de Tecnología
- Arquitecto de Tecnología
- Jefe de Seguridad
    - Administrador de Seguridad
    - Ingeniero de Seguridad
- Jefe de Riesgo
    - Administrador de Riesgo
    - Ingeniero de Riesgo.
- Jefe de Desarrollo o nuevos productos.
    - Administrador de desarrollo
    - Ingeniero de Desarrollo
- Jefe de Operaciones
    - Administrador de Operaciones
    - Ingeniero de Operaciones
- Jefe de Cambios.
    - Administrador de Cambios
- Jefe de Capacidad.
    - Administrador de capacidad
- Jefe de Continuidad.
    - Administrador de Continuidad

9.4 MEDICIÓN DE NIVEL DE MADUREZ

Con el fin de realizar una implementación del Marco estratégico de gestión para la continuidad de los servicios de TI, hemos formulado 2 tipos de encuestas que permitirán medir el estado actual de los distintos procesos de la organización, identificar las brechas y oportunidades tecnológicas.

Para evaluar el nivel de madurez de una institución universitaria privada colombiana, con respecto al marco estratégico de gestión de continuidad de los servicios de TI se crearon las siguientes preguntas que tienen como objetivo evaluar el nivel de implementación de las principales actividades de los diferentes subprocesos.

A continuación se lista el cuestionario con las preguntas:

Tabla 10.Criterios de evaluación nivel de madurez

Nombre	Pregunta
Gestionar el Marco de Gestión de TI	¿Se cuenta con una estructura de TI organizacional?
	¿Se cuentan con roles de TI establecidos?
	¿Se cumple con las políticas y procedimientos establecidos por el departamento de tecnología?
Gestionar la Estrategia	¿Se cuenta con un plan estratégico de tecnología definido?
	¿Es el plan estratégico de tecnología comunicado?
Gestionar los Acuerdos de Servicio	¿Se encuentran establecidos acuerdos de servicio para todos los servicios de tecnología?
	¿Son los acuerdos de servicio gestionados, revisados y modificados?
Gestionar el Riesgo	¿Se cuenta con un proceso de gestión de riesgos?
	¿Se Mantiene un perfil de riesgo, es este actualizado y comunicado a la alta gerencia?
	¿Se cuenta con un procedimiento de tratamiento de riesgos establecidos?
Gestionar la Seguridad	¿Se cuenta con un sistema de gestión de seguridad Informática?
	¿Existe un plan de tratamiento de riesgos dentro de la organización?

	¿Los roles y responsabilidades de los tratamientos de riesgos son establecidos?
Gestionar los Programas y Proyectos	¿Se cuenta con un proceso que involucra la planificación de los proyectos de tecnología?
	¿Se gestionan los riesgos asociados a los nuevos proyectos de tecnología?
	¿Se cuenta con actividades para la gestión de recursos de los proyectos?
Gestionar la Definición de Requisitos	¿Se cuenta con un proceso o actividades para la recolección y validación de requerimientos?
Gestionar la Identificación y la Construcción de Soluciones	¿Las soluciones entregadas por tecnología cuentan con un proceso de verificación de calidad?
Gestionar la Disponibilidad y la Capacidad	¿Las interrupciones del negocio son medidas y tratadas?
	¿Se cuenta con un plan de capacidad?
	¿Los incidentes de disponibilidad son medidos?
	¿Se cuenta con historia de los incidentes de disponibilidad y capacidad.
Gestionar los Cambios	¿Se cuenta con procedimientos que manejan el ciclo de vida de los componentes que hacen parte de la CMDB?
	¿Los cambios son controlados y requieren de aprobación por roles definidos por la dirección de tecnología?
Gestionar la Configuración	¿Se establecen modelos de configuración?
	¿Se cuenta con una CMDB?
Gestionar las Operaciones	¿Existe un procedimiento para la administración de las instalaciones de TI?
	¿Es la infraestructura de TI supervisada?
Gestionar las Peticiones y los Incidentes del Servicio	¿Se encuentra con un procedimiento para la atención de Peticiones, Incidentes de Servicio.
	¿Los incidentes son clasificados y priorizados?
	¿Se cuenta con una base de datos de peticiones e incidentes.
Gestionar la Continuidad	¿Se cuenta con un proceso para la gestión de la continuidad?
	¿Se cuenta con una política de continuidad?
	¿Se cuenta con una estrategia de continuidad?
	¿El plan de continuidad es probado y revisado?
	¿Se cuentan con acuerdos de respaldo?

Para la evaluación se adaptaron los siguientes criterios de evaluación como se muestra a continuación.

Tabla 11.Criterios de evaluación nivel de madurez

Nivel	Significado	Cumplimiento	Calificación
0	**Proceso Incompleto:** El Proceso no está Implementado	0%	0
1	**Proceso Ejecutado:** Proceso implementado alcanza su propósito	Entre 0% y 20%	1
2	**Proceso Gestionado:** Proceso ejecutado está implementado de forma gestionada	Entre 20% y 40%	2
3	**Proceso Establecido:** El proceso gestionado ahora está implementado usando un proceso definido	Entre 40% y 60%	3
4	**Proceso predecible:** El proceso establecido ahora se ejecuta dentro de límites definidos.	Entre 60% y 80%	4
5	**Proceso Optimizado:** El proceso predecible es mejorado de forma continua	Entre 80% y 100%	5

El procedimiento para la evaluación es como sigue:

- Se responde cada pregunta de 0 a 5 conforme la actividad o tarea cumpla con el nivel especificado.
- Al final se toma un promedio para cada proceso.
- Se determinan cuáles fueron las respuestas más bajas.
- Se plantean planes o tareas que aumenten el respectivo nivel.
- Cumplido el plan o las tareas, se vuelve a evaluar para determinar el nivel de madurez alcanzado.

10. CASO DE ESTUDIO

10.1 UNIVERSIDAD DEL NORTE

Actualmente la universidad del norte cuenta con procesos de planeación y prospectiva los cuales constituyen en pilares fundamentales de calidad, y se han convertido en una fortaleza importante en la toma de decisiones en la gestión universitaria.

Se establecen planes de desarrollo que abarcan objetivos y estrategias para los próximos 5 años.

La Dirección de Tecnología Informática y de Comunicaciones (DirTic) como unidad organizacional apoya mediante sus objetivos y estrategias horizontalmente y verticalmente a la organización.

Aunque los objetivos y estrategias de la DirTic se encuentran alineados con los del negocio, no existe actualmente un marco de gobierno de tecnología claro, por lo anterior, es una prioridad para los próximos años establecerlo.

Los actuales indicadores de gestión de TI fueron establecidos teniendo en cuenta algunos marcos de referencia y se encuentran bajo el Sistema Integrado de Gestión de Calidad de la universidad, basado en la norma ISO 9001:2015.

10.1.1 Caracterización Organización

10.1.1.1 Misión

La Fundación Universidad del Norte, acorde con los principios, valores y objetivos que la guían desde su creación, tiene como misión la formación integral de la persona en el plano

de la educación superior, y la contribución, mediante su presencia institucional en la comunidad, al desarrollo armónico de la sociedad y del país, especialmente de la Región Caribe colombiana.

La Fundación cumple esta labor universitaria tanto en la modalidad de pregrado como en la formación avanzada, caracterizándose su quehacer por un amplio contenido social y humanístico, y por el énfasis en la fundamentación científica e investigativa para responder a los requerimientos del progreso de la ciencia y a las necesidades sociales de la región y del país.

Busca la Institución formar a sus estudiantes como personas pensantes, analíticas y de sólidos principios éticos, que conciban ideas innovadoras a fin de que participen de manera activa, emprendedora, responsable, honesta, crítica y pragmática en el proceso de desarrollo social, económico, político y cultural de la comunidad.

La Universidad propende porque la formación que en ella se imparte se realice con profesorado idóneo, calificado y con profunda vocación académica. Para apoyarlos en esa tarea, está decidida a contar con los métodos de enseñanza, de investigación y de extensión más adecuados y avanzados de la educación superior contemporánea. En este sentido, la ciencia, la tecnología, las humanidades y las artes seguirán siendo los ejes institucionales distintivos para la formación del estudiante.

Presente en la vida de la comunidad mediante el ejercicio de sus funciones académicas (docencia, investigación, extensión y servicios al sector externo), la Universidad del Norte procura que sus directivos, profesores, estudiantes y exalumnos se mantengan en permanente estudio, análisis e investigación de los problemas concretos de la comunidad en que se encuentran.

Nuestra institución está comprometida desde sus orígenes, en el presente y hacia el futuro, con todas las dimensiones del desarrollo social, económico, político, ambiental y cultural, con responsabilidad social, manteniéndose en su lugar propio de inserción en la sociedad, que es el académico.[6]

10.1.1.2 Visión

En el año 2022, la Universidad del Norte seguirá siendo una de las mejores universidades del país, de América Latina y el Caribe, por su compromiso con la excelencia en la formación de sus estudiantes y en la creación del conocimiento, su alto impacto en el desarrollo, regional y nacional, y el diálogo con la sociedad global en la búsqueda continua de un futuro mejor.

En la realización de visión a 2022, la universidad fortalecerá sus acreditaciones, su posicionamiento en los rankings internacionales como reconocimiento a la excelencia en los procesos de enseñanza-aprendizaje con innovación y pedagogía, el alto nivel científico de su cuerpo profesoral y la proyección internacional de la extensión.

Incrementará y dinamizará la competitividad de sus egresados, quienes serán aliados estratégicos en la ejecución de proyectos y en el fortalecimiento de los vínculos con el sector empresarial.

[6] Misión y Visión de Uninorte. https://www.uninorte.edu.co/web/sobre-nosotros/mision-vision

10.1.1.3 Gobierno Corporativo

La Universidad del Norte en cuanto al Gobierno Institucional está regido por su máxima autoridad, el Consejo Directivo que se encarga de establecer las políticas generales que rigen a la institución, a su vez que ejerce las tareas de Evaluación, Supervisión y Medición a nivel institucional.

En la siguiente figura encontrará el organigrama actual de la Universidad del Norte.

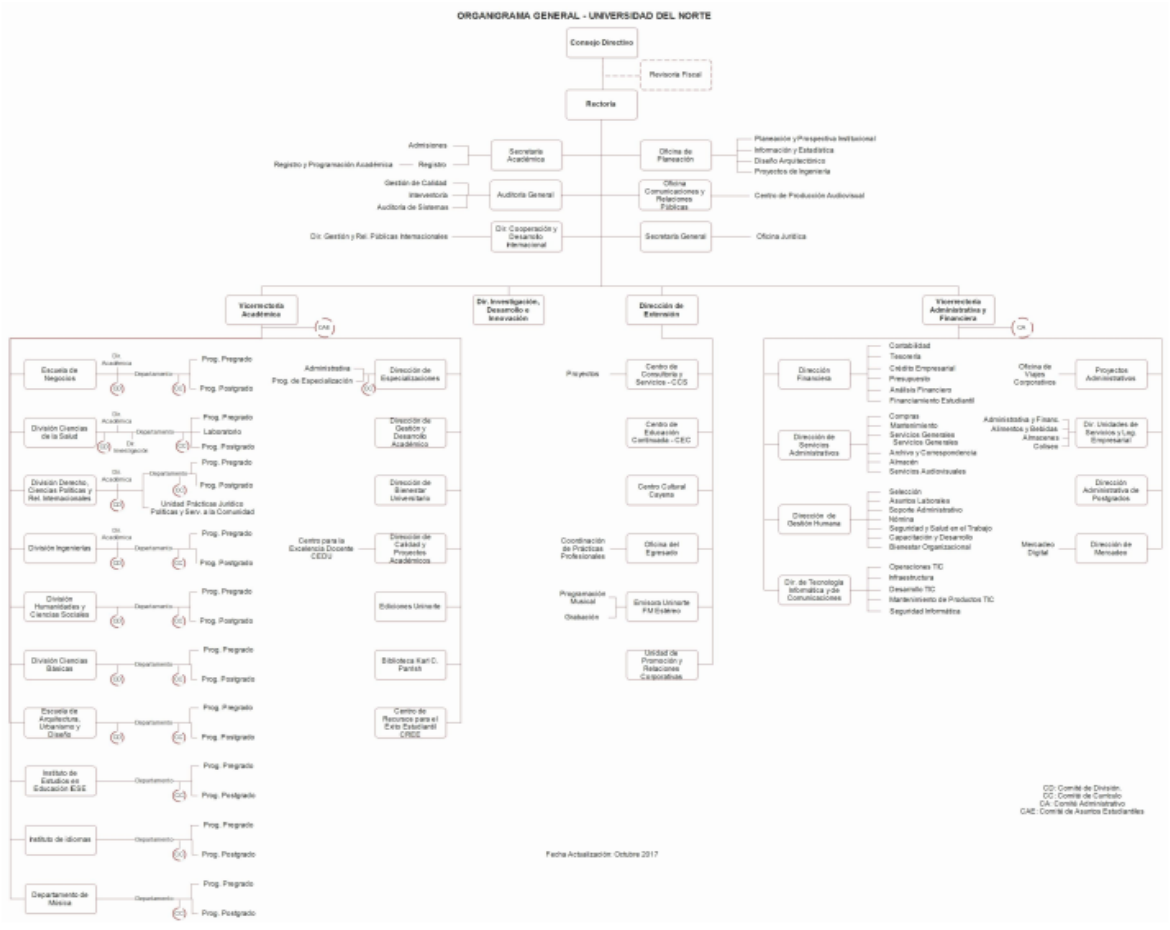


Figura 6. Organigrama de la Universidad del Norte[7]

[7] Tomado de https://www.uninorte.edu.co/web/sobre-nosotros/organigrama

10.1.1.4 Estado Actual de GyG-TI

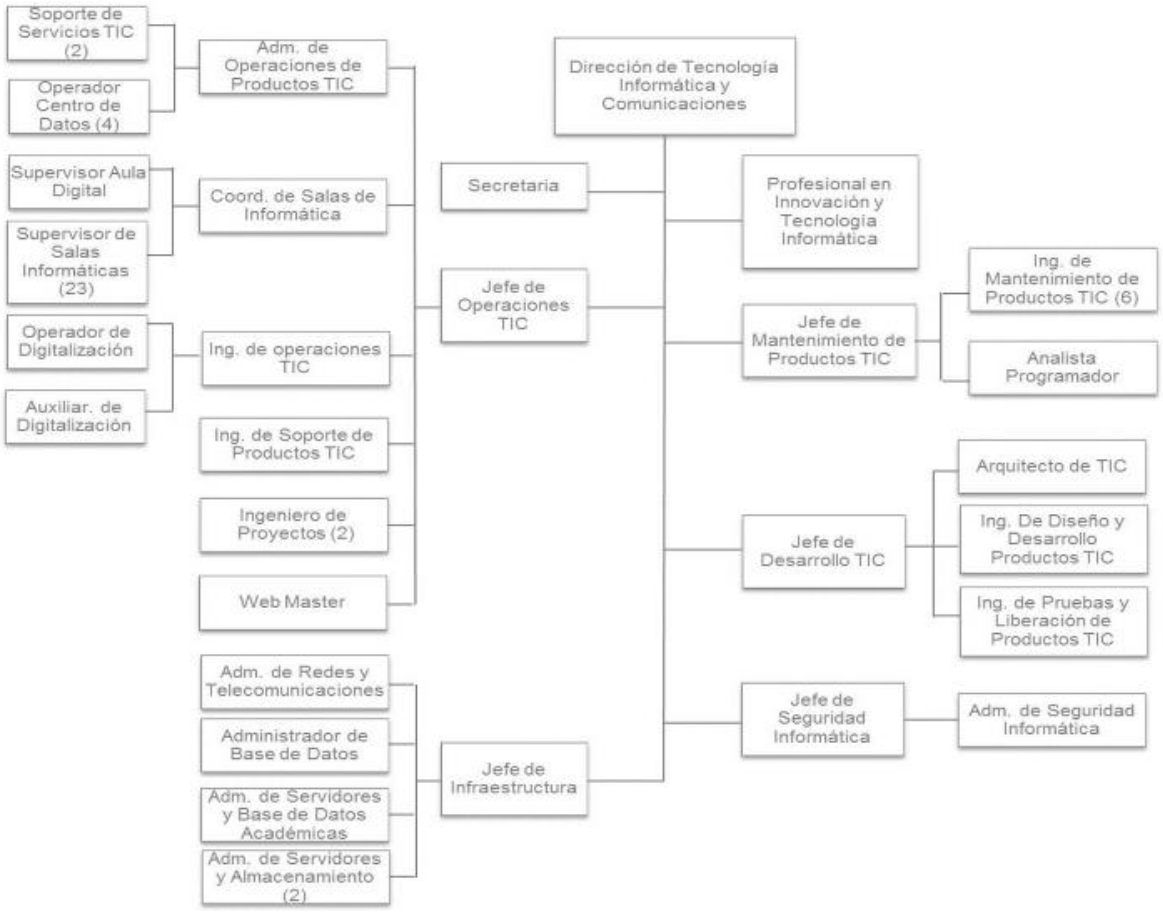


Figura 7. Organigrama de la Dirección de TI de la Universidad del Norte[8]

La Gestión de Tecnología Informática y de Comunicaciones involucra el desarrollo, mantenimiento y operación de servicios institucionales basados en el uso de la tecnología de información y de comunicación (TIC), así como la actualización de la infraestructura

[8] https://www.uninorte.edu.co/web/gestion-administrativa-y-financiera/direccion-de-tecnologia-informatica-y-de-comunicaciones

tecnológica y el entrenamiento a los usuarios en el aprovechamiento de estos recursos y servicios.

En este sentido, la gestión de la tecnología informática y de comunicaciones es muy importante para el logro de los objetivos institucionales, adoptando tecnologías y estándares de acuerdo con el desarrollo de las tendencias mundiales, que faciliten la prestación de servicios de una manera ágil y oportuna y promuevan la calidad y seguridad de los mismos.

La tecnología informática y de comunicaciones seguirá siendo un sello diferenciador para mantener a la Universidad del Norte en posición de liderazgo en su conocimiento, apropiación y utilización en el ejercicio de la función académica y administrativa.

El área de Tecnología Informática y de Comunicaciones tiene como visión ser el socio estratégico para el logro de los objetivos institucionales, adoptando tecnologías y estándares de TI acordes con las tendencias mundiales, que permitan la implementación de servicios ágiles y oportunos; garantizando la calidad, seguridad y efectividad de los mismos.

Funciones

- Responder por la planeación, adquisición, actualización, implementación, operación y calidad de la infraestructura, procesos y productos relacionados con la tecnología informática y de comunicaciones; cuidando que las inversiones requeridas signifiquen un menor costo y un mayor beneficio institucional.
- Definir estrategias y procesos que garanticen la disponibilidad, confiabilidad, confidencialidad, integridad, eficiencia y eficacia de los productos TIC y de la infraestructura tecnológica sobre la cual operan.

- Participar, junto con la Vicerrectoría Administrativa y Financiera, en la definición de políticas de desarrollo y seguridad en el área de informática y comunicaciones.
- Definir planes e implementar mediciones para el aseguramiento de la calidad de los productos, servicios y procesos de la Gestión de Tecnología Informática y de Comunicaciones.
- Evaluar y aprobar la adopción de nuevas tecnologías, marcos de referencia y mejores prácticas relacionadas con la implementación, operación y soporte de los servicios de tecnología informática y de comunicaciones.

Procesos

La Dirección de tecnología informática y de Comunicaciones está conformada por cinco procesos que se encuentran bajo la norma ISO 9001:2015. Los procesos que hacen parte de la dirección son:

- Analizar e implementar nuevos productos TIC
- Activar y o desactivar servicios TIC
- Suministrar mantenimiento a los productos e infraestructura TIC
- Gestión de operación TIC
- Gestión de infraestructura TIC

Fortalezas y debilidades

La Dirección de Tecnología informática y de comunicaciones tiene como gran fortaleza que sus procesos están alineados a las buenas prácticas de ITIL, lo que le permite tener

un mejor control y seguimiento del ciclo de vida del servicio de los productos TIC que se soportan.

Cuenta con una mesa de servicios “Centro de Soluciones Uninorte” establecida hace 9 años, en donde los usuarios reportan sus incidentes o solicitudes de servicio, tiene establecido claramente especificaciones de servicio para cada tipo de producto TIC, roles y métricas que le permiten constantemente evaluar y mejorar el proceso para lograr aumentar la satisfacción de los usuarios.

En cuanto a las debilidades, actualmente la Dirección de Tecnología Informática y de Comunicaciones no cuenta con un gobierno y gestión de TI implementado.

10.2 MEDICIÓN DE MADUREZ DE LA ORGANIZACIÓN DEL MODELO PROPUESTO

10.2.1 Medición de la madurez inicial

Al aplicar la medición de madurez del MEGCS en la Universidad del Norte se tuvieron los siguientes resultados. En el anexo 1 se muestra el cuestionario diligenciado con todas sus respuestas.

Proceso	Valoración
Gestionar el Marco de Gestión de TI	4
Gestionar la Estrategia	4
Gestionar los Acuerdos de Servicio	5
Gestionar el Riesgo	3,3
Gestionar la Seguridad	3,7

Gestionar los Programas y Proyectos	3,7
Gestionar la Definición de Requisitos	3
Gestionar la Identificación y la Construcción de Soluciones	4
Gestionar la Disponibilidad y la Capacidad	4,5
Gestionar los Cambios	3
Gestionar la Configuración	2,5
Gestionar las Operaciones	4
Gestionar las Peticiones y los Incidentes del Servicio	4,3
Gestionar la Continuidad	1,6
PROMEDIO	***3,6***

Tabla 12.Evaluación inicial Uninorte

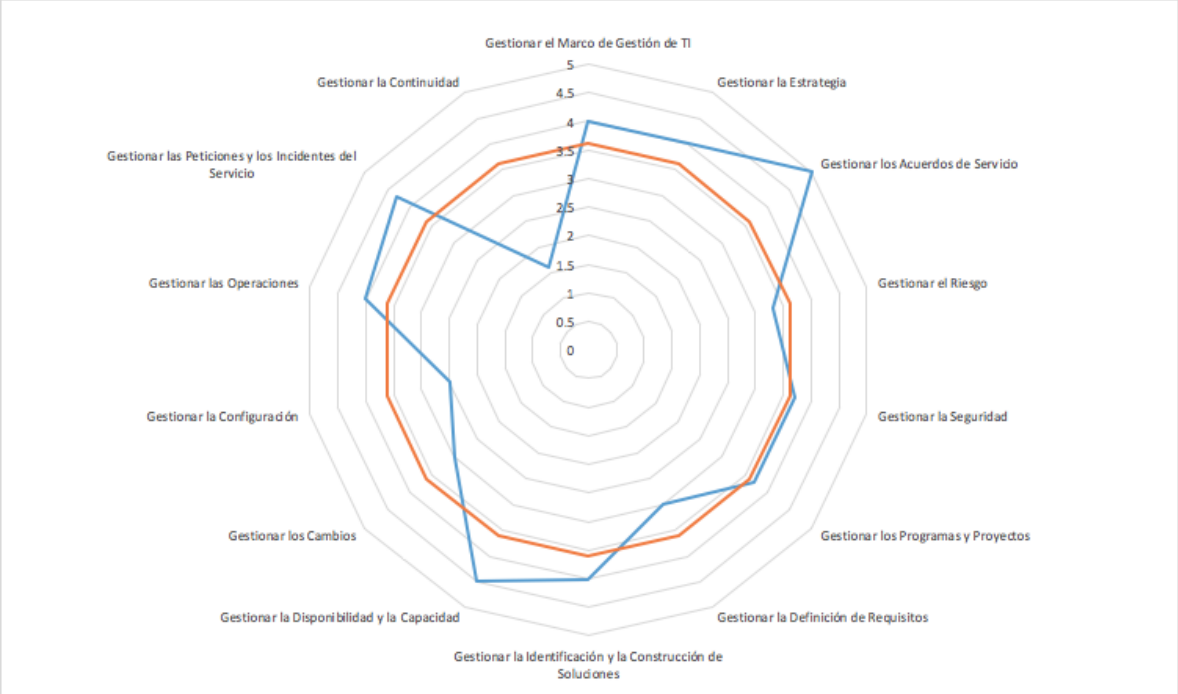


Figura 8. Medición de madurez inicial

10.2.2 Análisis de brechas evaluación inicial

Para poder proponer el plan de trabajo inicial se tendrá en cuenta todos los proceso cuyo puntaje fue el menor a tres (3).

Se propone este el siguiente plan de trabajo inicial:

Actividades	Inicio	Fin
Diseñar el proceso de gestión de la continuidad con base en las actividades del modelo propuesto.	1/2019	2/2019
Establecer la estructura organizacional necesaria para soportar el proceso de continuidad, establecer los roles de Jefe de Continuidad, Administrador de Continuidad dentro de la organización	2/2019	5/2019
Implementar los indicadores de gestión de continuidad del modelo propuesto	2/2019	5/2019
Diseñar una estrategia de continuidad de negocio	2/2019	5/2019
Diseñar un plan de continuidad de Negocio	2/2019	5/2019
Establecer dentro proceso actual de gestión de la configuración actividades que permitan mantener el ciclo de vida de la CMDB, el cual contemple la creación de modelos de configuración que puedan ser reutilizados, revisados y utilizados.	1/2019	2/2019
Establecer un comité de continuidad que permita establecer las acciones necesarias para la implementación del plan de continuidad	3/2019	3/2019
Implementar un Sistema de Gestión de seguridad informática	1/2019	1/2020
Revisar, actualizar los acuerdos de respaldo existentes dentro de la organización.	1/2019	2/2019
Implementar métricas del modelo propuesto para el proceso de gestión de requisitos	1/2019	2/2019

10.2.3 Medición de la madurez después de la aplicación del plan de trabajo inicial

Al aplicar la medición de madurez del MEGCS en la Universidad del Norte después de ela aplicación del plan de trabajo inicial, se tuvieron los siguientes resultados. En el anexo 2 se muestra el cuestionario diligenciado con todas sus respuestas.

Proceso	Valoración
Gestionar el Marco de Gestión de TI	4
Gestionar la Estrategia	4
Gestionar los Acuerdos de Servicio	5
Gestionar el Riesgo	3,7
Gestionar la Seguridad	4
Gestionar los Programas y Proyectos	3,7
Gestionar la Definición de Requisitos	4
Gestionar la Identificación y la Construcción de Soluciones	4
Gestionar la Disponibilidad y la Capacidad	4,5
Gestionar los Cambios	4
Gestionar la Configuración	4
Gestionar las Operaciones	4
Gestionar las Peticiones y los Incidentes del Servicio	4,3
Gestionar la Continuidad	3,6
PROMEDIO	***4,1***

Tabla 13. Evaluación posterior Uninorte

Se puede notar que el nivel de madurez después de la aplicación del plan de trabajo proporciona mejoras a los procesos Gestión de Riesgos, Gestión de seguridad, Gestionar la

definición de requisitos, Gestionar los cambios, Gestionar la configuración y notablemente el proceso de Gestión de la continuidad.

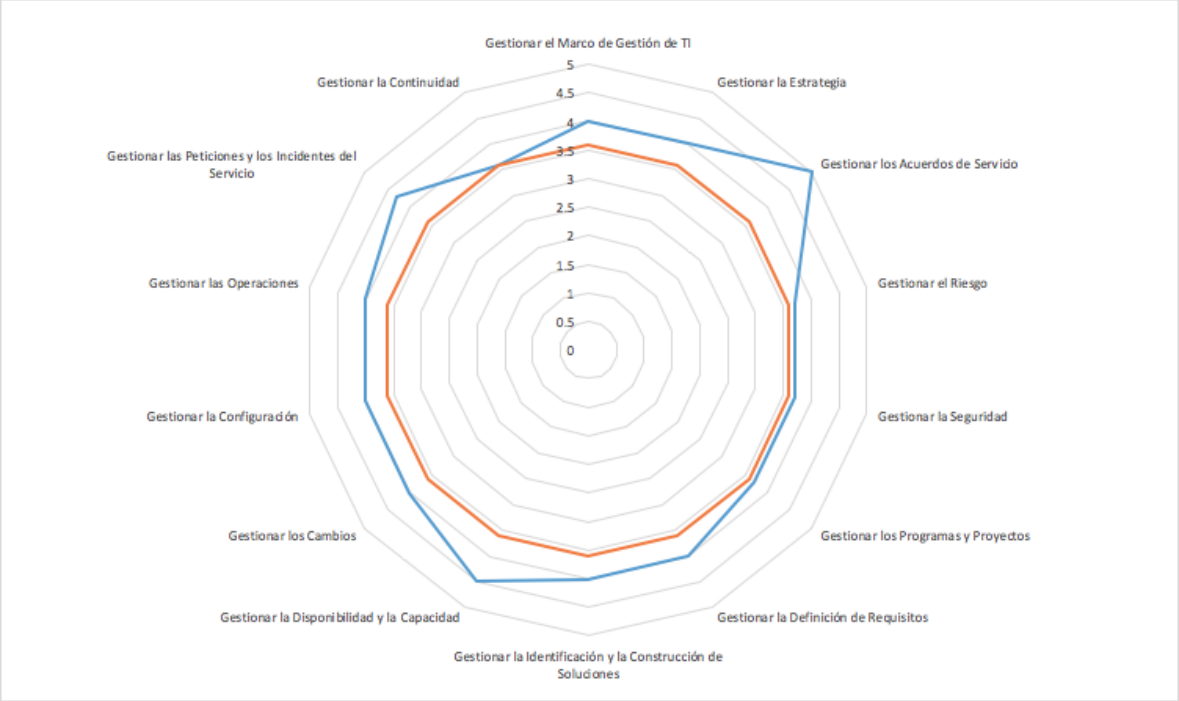


Figura 9. Medición de madurez después del plan de trabajo inicial

1. CONCLUSIONES

- Las instituciones universitarias privadas colombianas debido al alto uso de las tecnologías para el soporte de sus procesos críticos están obligadas a implementar un Gobierno y Gestión de TI que a su vez permita gestionar las estrategias planteadas eficazmente.
- Aunque para las instituciones universitarias privadas en Colombia no sea obligatorio, deben implementar buenas prácticas (COBIT 5, ITIL) que permitan establecer controles para garantizar la continuidad de los servicios de TI de la institución.
- Con la implementación de los proyectos y actividades propuestos se evidencia que se pueden cerrar las brechas en el baseline establecido.

BIBLIOGRAFÍA

Swanson, Bowen, Phillips, Gallup, Lynes (2010) NIST Special Publication 800-34 Rev. 1 National Institute of Standards and Technology. The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning Disponible: *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf*

Weill, Peter, Ross Jeanne. IT Governance. Harvard Business School Press (2004). Ciudad: Boston USA, Páginas 85-117.

Fernandez, Antonio,. Gobierno de TI para las universidades. Conferencia de Rectores de las Universidades Españolas (CRUE) (2012). Ciudad: Madrid España, Páginas 10-101.

Rodriguez, Alberto, Vargas, Maria (2016). Modelo de un sistema de gestión de continuidad del negocio para microfinanciera basado en la ISO/IEC 22301 y en la circular G-139-2009 de la SBS, Disponible: http://repositorioacademico.upc.edu.pe/upc/bitstream/10757/620834/1/Cespedes_VK_Soto_RL.pdf

Gomez, Maury (2013) Diseño de un marco metodológico para la implementación de una estrategia de respaldo de información. Disponible: http://repositorio.cuc.edu.co/xmlui/bitstream/handle/11323/145/TESIS.pdf?sequence=1

ISACA. (2011) COBIT 5: The Framework. COBIT 5 - An ISACA Framework, pp. 1–85., Disponible: www.isaca.org/Knowledge-Center/Research/Documents/COBIT5-Framework-ED-27June2011.pdf.

OGC. (2017) ITIL® - What Is ITIL? *ITIL® Home*. APM Group Ltd., n.d. Web.

ANEXO 1. FORMULARIO EVALUACIÓN INICIAL UNINORTE

Nombre	Pregunta	Valoración	
Gestionar el Marco de Gestión de TI	¿Se cuenta con una estructura de ti organizacional?	4	4
	¿Se cuentan con roles de ti establecidos?	4	
	¿Se cumple con las políticas y procedimientos establecidos por el departamento de tecnología?	4	
Gestionar la Estrategia	¿Se cuenta con un plan estratégico de tecnología definido?	4	4
	¿Es el plan estratégico de tecnología comunicado?	4	
Gestionar los Acuerdos de Servicio	¿Se encuentran establecidos acuerdos de servicio para todos los servicios de tecnología?	5	5
	¿Son los acuerdos de servicio gestionados, revisados y modificados?	5	
Gestionar el Riesgo	¿Se cuenta con un proceso de gestión de riesgos?	3	3,3
	¿Se Mantiene un perfil de riesgo, es este actualizado y comunicado a la alta gerencia?	3	
	¿Se cuenta con un procedimiento de tratamiento de riesgos establecidos?	4	
Gestionar la Seguridad	¿Se cuenta con un sistema de gestión de seguridad Informática?	2	3,7
	¿Existe un plan de tratamiento de riesgos dentro de la organización?	5	
	¿Los roles y responsabilidades de los tratamientos de riesgos son establecidos?	4	
Gestionar los Programas y Proyectos	¿Se cuenta con un proceso que involucra la planificación de los proyectos de tecnología?	5	3,7
	¿Se gestionan los riesgos asociados a los nuevos proyectos de tecnología?	3	
	¿Se cuenta con actividades para la gestión de recursos de los proyectos?	3	
Gestionar la Definición de Requisitos	¿Se cuenta con un proceso o actividades para la recolección y validación de requerimientos?	3	3

Gestionar la Identificación y la Construcción de Soluciones	¿Las soluciones entregadas por tecnología cuentan con un proceso de verificación de calidad?	4	4
Gestionar la Disponibilidad y la Capacidad	¿Las interrupciones del negocio son medidas y tratadas?	4	4,5
	¿Se cuenta con un plan de capacidad?	4	
	¿Los incidentes de disponibilidad son medidos?	5	
	¿Se cuenta con historia de los incidentes de disponibilidad y capacidad.	5	
Gestionar los Cambios	¿Se cuenta con procedimientos que manejan el ciclo de vida de los componentes que hacen parte de la CMDB?	3	3
	¿Los cambios son controlados y requieren de aprobación por roles definidos por la dirección de tecnología?	3	
Gestionar la Configuración	¿Se establecen modelos de configuración?	2	2,5
	¿Se cuenta con una CMDB?	3	
Gestionar las Operaciones	¿Existe un procedimiento para la administración de las instalaciones de TI?	4	4
	¿Es la infraestructura de TI supervisada?	4	
Gestionar las Peticiones y los Incidentes del Servicio	¿Se encuentra con un procedimiento para la atención de Peticiones, Incidentes de Servicio.	4	4,3
	¿Los incidentes son clasificados y priorizados?	5	
	¿Se cuenta con una base de datos de peticiones e incidentes.	4	
Gestionar la Continuidad	¿Se cuenta con un proceso para la gestión de la continuidad?	1	1,6
	¿Se cuenta con una política de continuidad?	1	
	¿Se cuenta con una estrategia de continuidad?	2	
	¿El plan de continuidad es probado y revisado?	1	
	¿Se cuentan con acuerdos de respaldo?	3	
Promedio:			**3,6**

ANEXO 2. FORMULARIO EVALUACIÓN POSTERIOR AL PLAN DE TRABAJO UNINORTE

Nombre	Pregunta	Valoración	
Gestionar el Marco de Gestión de TI	¿Se cuenta con una estructura de ti organizacional?	4	4
	¿Se cuentan con roles de ti establecidos?	4	
	¿Se cumple con las políticas y procedimientos establecidos por el departamento de tecnología?	4	
Gestionar la Estrategia	¿Se cuenta con un plan estratégico de tecnología definido?	4	4
	¿Es el plan estratégico de tecnología comunicado?	4	
Gestionar los Acuerdos de Servicio	¿Se encuentran establecidos acuerdos de servicio para todos los servicios de tecnología?	5	5
	¿Son los acuerdos de servicio gestionados, revisados y modificados?	5	
Gestionar el Riesgo	¿Se cuenta con un proceso de gestión de riesgos?	4	3,7
	¿Se Mantiene un perfil de riesgo, es este actualizado y comunicado a la alta gerencia?	3	
	¿Se cuenta con un procedimiento de tratamiento de riesgos establecidos?	4	
Gestionar la Seguridad	¿Se cuenta con un sistema de gestión de seguridad Informática?	3	4

	¿Existe un plan de tratamiento de riesgos dentro de la organización?	5	
	¿Los roles y responsabilidades de los tratamientos de riesgos son establecidos?	4	
Gestionar los Programas y Proyectos	¿Se cuenta con un proceso que involucra la planificación de los proyectos de tecnología?	5	3,7
	¿Se gestionan los riesgos asociados a los nuevos proyectos de tecnología?	3	
	¿Se cuenta con actividades para la gestión de recursos de los proyectos?	3	
Gestionar la Definición de Requisitos	¿Se cuenta con un proceso o actividades para la recolección y validación de requerimientos?	4	4
Gestionar la Identificación y la Construcción de Soluciones	¿Las soluciones entregadas por tecnología cuentan con un proceso de verificación de calidad?	4	4
Gestionar la Disponibilidad y la Capacidad	¿Las interrupciones del negocio son medidas y tratadas?	4	4,5
	¿Se cuenta con un plan de capacidad?	4	
	¿Los incidentes de disponibilidad son medidos?	5	
	¿Se cuenta con historia de los incidentes de disponibilidad y capacidad.	5	

Gestionar los Cambios	¿Se cuenta con procedimientos que manejan el ciclo de vida de los componentes que hacen parte de la CMDB?	4	4
	¿Los cambios son controlados y requieren de aprobación por roles definidos por la dirección de tecnología?	4	
Gestionar la Configuración	¿Se establecen modelos de configuración?	4	4
	¿Se cuenta con una CMDB?	4	
Gestionar las Operaciones	¿Existe un procedimiento para la administración de las instalaciones de TI?	4	4
	¿Es la infraestructura de TI supervisada?	4	
Gestionar las Peticiones y los Incidentes del Servicio	¿Se encuentra con un procedimiento para la atención de Peticiones, Incidentes de Servicio.	4	4,3
	¿Los incidentes son clasificados y priorizados?	5	
	¿Se cuenta con una base de datos de peticiones e incidentes.	4	
Gestionar la Continuidad	¿Se cuenta con un proceso para la gestión de la continuidad?	4	3,6
	¿Se cuenta con una política de continuidad?	4	
	¿Se cuenta con una estrategia de continuidad?	4	
	¿El plan de continuidad es probado y revisado?	2	
	¿Se cuentan con acuerdos de respaldo?	4	
Promedio:			4,1